BLOCK CHAIN PRACTICE

区块链实战

吴为◎著

数字货币、金融、物联网、大数据、医疗、教育、公证等七大领域应用实例

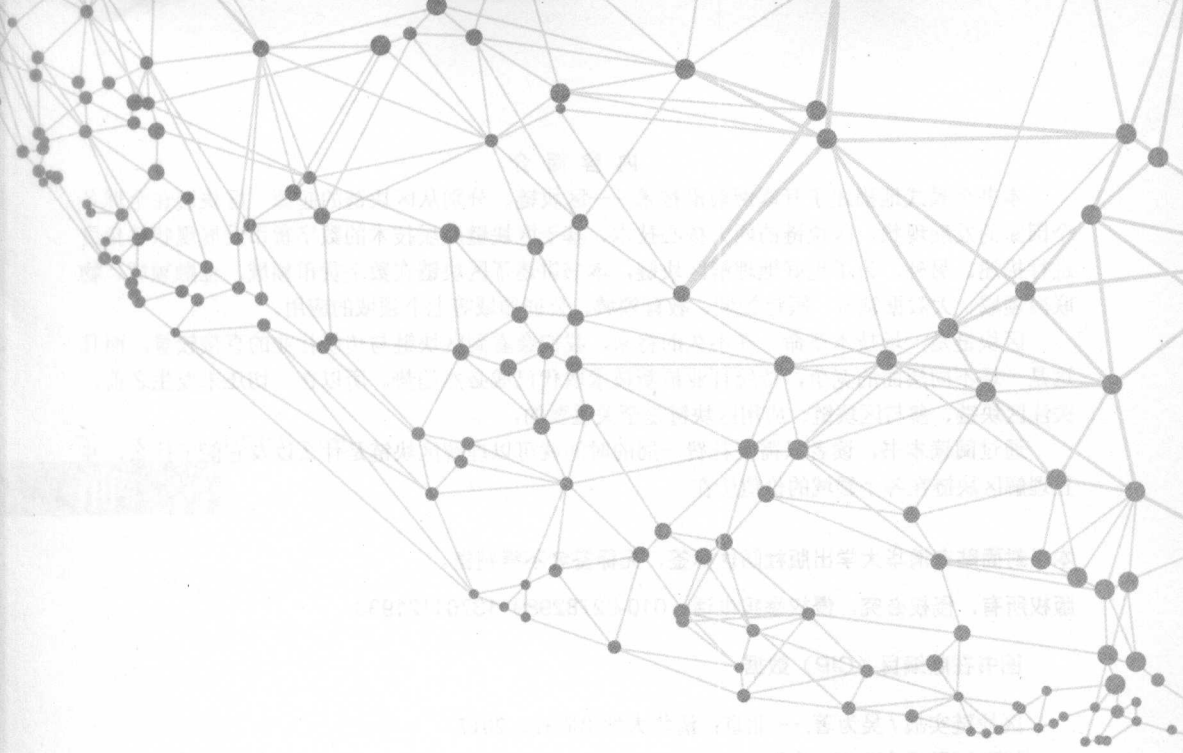
为了不被时代淘汰，请用一周时间，读懂区块链

清華大學出版社

本书全景式地描述了互联网前沿技术——区块链，分别从区块链的起源、区块链在全球各个国家的发展现状、区块链的四大核心技术、基于区块链底层技术的数字货币发展现状等角度进行描述。另外，为了更好地理解区块链，本书讲述了区块链在数字货币领域、金融领域、物联网领域、大数据领域、医疗领域、教育领域、公证领域等七个领域的应用。

区块链是一场技术革命。在不久的将来，我们会看到区块链与传统行业的直接较量。而且这是一场不同层面的竞争，传统行业被新技术取代已成必然趋势。所以在一切还未发生之前，关注区块链、参与区块链、应用区块链是至关重要的。

通过阅读本书，读者只需要花费一周的时间就可以理解区块链是什么以及它能干什么，并且理解区块链在各个领域的价值所在。



BLOCK CHAIN PRACTICE

区块链实战

吴为◎著

清華大學出版社
北京

内 容 简 介

本书全景式地描述了互联网前沿技术——区块链，分别从区块链的起源、区块链在全球各个国家的发展现状、区块链的四大核心技术、基于区块链底层技术的数字货币发展现状等角度进行描述。另外，为了更好地理解区块链，本书讲述了区块链在数字货币领域、金融领域、物联网领域、大数据领域、医疗领域、教育领域、公证领域等七个领域的应用。

区块链是一场技术革命。在不久的将来，我们会看到区块链与传统行业的直接较量。而且这是一场不同层面的竞争，传统行业被新技术取代已成必然趋势。所以在一切还未发生之前，关注区块链、参与区块链、应用区块链是至关重要的。

通过阅读本书，读者只需要花费一周的时间就可以理解区块链是什么以及它能干什么，并且理解区块链在各个领域的价值所在。

图书在版编目（CIP）数据

区块链实战 / 吴为著. — 北京：清华大学出版社，2017
ISBN 978-7-302-47589-7

Ⅰ. ①区… Ⅱ. ①吴… Ⅲ. ①电子商务－支付方式－研究 Ⅳ. ①F713.361.3

中国版本图书馆 CIP 数据核字（2017）第 146671 号

责任编辑： 刘 洋
封面设计： 李召霞
版式设计： 方加青
责任校对： 王凤芝
责任印制： 王静怡

出版发行： 清华大学出版社
网 址：http://www.tup.com.cn，http://www.wqbook.com
地 址：北京清华大学学研大厦 A 座 邮 编：100084
社 总 机：010-62770175 邮 购：010-62786544
投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn
质 量 反 馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
印 装 者： 三河市金元印装有限公司
经 销： 全国新华书店
开 本： 170mm×240mm **印 张：** 14.75 **字 数：** 262 千字
版 次： 2017 年 9 月第 1 版 **印 次：** 2017 年 9 月第 1 次印刷
定 价： 49.00 元

产品编号：075513-01

Block chain practice

前 言

2017 年 2 月，中国人民银行（简称央行）研究并测试数字票据交易平台的事件轰动了全球，该数字票据交易平台应用的基础技术就是区块链。此外，央行旗下数字货币研究所也在 2017 年上半年正式挂牌成立。这意味着中国人民银行成为全球范围内首个研究数字货币并将数字货币应用于真实生活的中央银行，并率先探索区块链技术在货币发行领域的应用。

那么，央行建立区块链数字票据交易平台对我们的现实生活会产生很大影响吗？答案是肯定的，大家可以想象一下：两三年以后，过年发红包不再是纸质钞票，而是一串串的数字密码，我们可以通过发送邮件、复制到 U 盘里或者通过手机直接将其发送给他人。

关于央行开发数字货币的原因，央行参事盛松成称：“未来的央行数字货币会从多个方面倒逼金融基础设施建设，让我国支付体系进一步完善，支付结算效率进一步提升。更值得一提的是，央行数字货币最后可以构成大数据系统，使经济交易活动的便利性和透明度进一步得到提高，这将有利于货币政策的有效运行和传导。”

在央行的积极带动下，我国各方资本纷纷在区块链行业布局。截至 2016 年年年底，平安银行、招商银行、民生银行都已经加入 R3 区块链联盟。截至 2017 年年初，我国 A 股市场上切入区块链概念的公司已经有 24 家，大部分公司是软件和信息技术提供商。

各大行业巨头公司也不甘落后。其中，万向集团建立了区块链实验室，华为加入了 Linux 基金会领导的超级账本区块链项目。另外，百度、光大投资管理公

司、中金甲子、宜信等机构向一家美国比特币初创公司投资了 6 000 万美元。

从全球范围来看，包括纳斯达克、花旗、Visa 在内的金融行业大咖也向区块链领域大把大把地砸钱，它们联合投资了一家区块链初创公司 Chain，涉及金额高达 3 000 万美元；花旗、摩根大通等金融机构还向一家区块链初创公司 Digital Asset 投资 5 000 万美元。

如今，各方都对区块链表示出极大的关注度，区块链技术正在从一片巨大的蓝海转变为一片巨大的红海。那么，区块链凭借什么魅力受到了全球关注呢？以金融业票据清算系统为例，区块链将从以下四个方面发挥作用。

第一，消除了票据中介角色。在应用了区块链技术之后，票据价值可以实现 P2P 无形传递，既不需要特定实物作为连接双方取得信任的证明，也不需要第三方对交易双方价值传递的信息做监督和验证。另外，票据交易双方常常需要通过票据中介来解决信息不对称问题，而借助区块链实现 P2P 交易后，票据中介的现有职能将被消除。

第二，防范票据市场风险。不透明、不规范以及高杠杆错配等潜规则使票据市场的风险频发，参与机构的多样性和逐利性也加大了这一风险。而区块链技术全网公开、数据不可篡改的特性可以防范道德风险；分布式系统无须第三方中介的特性完全避免了人为操作风险；自动控制参与者资产和负债两端平衡且数据公开透明的特性有利于控制市场风险。

第三，建立去中心分布模式的电子商业汇票系统。现有的电子商业汇票系统（Electronic Commercial Draft System，ECDS）是一个中心化系统，其中心为央行，其他银行和企业通过直连或网银代理的方式接入央行的中心化登记和数据交换系统。区块链技术将会改变现有电子商业汇票系统的存储和传输结构，建立去中心分布式模式，还能利用时间戳完整反映票据从产生到毁灭的过程，使每一张票据都可以追溯历史。区块链建立的全新连续“背书”机制将更加真实地反映票据权利的转移过程。

第四，降低了市场监管成本。多样的操作方式使得票据市场的监管变得非常繁杂。监管方式也只能是现场审核，而业务模式和流转则没有全流程的快速审查和调阅手段。

区块链的价值具有无限潜力，不仅仅是在重构票据清算系统方面，也不仅仅是在金融领域。而且区块链红海席卷全球的局势已经基本建立，各种利好也即将降临，那些提前进入区块链行业，提供建设区块链经济最原始资本的人，注定会率先品尝到区块链带来的丰厚回报。

本书特色

1. 内容全面，结构清晰

本书内容包括区块链的起源、发展、应用以及趋势预测，并重点讲述了区块链在金融领域、物联网领域、大数据领域、医疗领域、教育领域以及公证领域的应用。而且全书架构清晰，有助于读者形成框架形式的认知。

2. 案例丰富，实战性强

本书加入很多真实且具有代表性的案例，使内容更加生动有趣。而且案例的加入使理论知识不再枯燥无味，读者更容易接受其中的观点。另外，本书理论与实战相结合，非常适合没有接触过区块链的读者阅读，帮助他们快速入门，深入理解区块链的价值。

3. 语言通俗，更接地气

新概念、新技术类的图书总是被作者包装得高大上，看起来非常有范儿，但实质上却提高了读者的理解门槛。而本书倾向于采用通俗易懂的语言为读者解读深奥的理论，让读者轻松理解与区块链相关的理论、应用等知识。

本书内容及体系结构

第 1 章：讲述了区块链起源于比特币，并对比特币的发行规律、价格变化等作出详细报告，有助于读者理解区块链与比特币的关系。

第 2 章：讲述区块链在人类世界的发展现状，包括各国政府对区块链的积极态度、全国各大企业对区块链应用的投资以及 2017 年最热门的 5 家区块链初创公司。

第 3 章：介绍了区块链的四大核心技术，包括具有去中心化创新、数据高度透明、不依赖信任以及信息可回溯性四大特征的分布式账本技术，用户掌握私钥以及匿名的非对称加密和授权技术，参与者共同维护的共识机制、自动控制，以及自动执行数字承诺的智能合约。

第 4 章：讲述了货币的进化历史以及当前三大数字货币（比特币、以太坊和莱特币）的发展现状，还将比特币与以太坊、莱特币作对比，帮助读者了解各自优势。

第 5 ～ 10 章：分别讲述了区块链在金融领域、物联网领域、大数据领域、医疗领域、教育领域以及公证领域的应用，帮助读者对区块链的价值形成系统

认识。

第 11 章：讲述了区块链技术与物联网、大数据、人工智能等领域深度融合的发展趋势，并分析了区块链将会颠覆传统行业、改变人类世界的发展前景。

本书读者对象

- 各领域企业领导、高管
- 金融科技企业工作人员
- 数字货币相关公司工作人员
- 区块链研究以及开发者
- 对区块链以及数字货币感兴趣的其他人群

参与本书编写工作的人员还有梁萍、李改霞、赵丹丹、李恬、曾丽佳、李雪霞、李卫霞、李艳霞、李伟光、李晓青、游万梅、贾云叶、宋佳佳、龚毅、梁现丽、王逊、鲁宗保、李小菊等。

编者

2017 年 5 月

Block chain practice

目 录

第 1 章　区块链起源

第 2 章　区块链——必将颠覆人类世界

第3章 区块链四大核心技术

第 4 章 区块链与数字货币

第 5 章 区块链在金融领域的应用

第 6 章　区块链在物联网领域的应用

第 7 章　区块链在大数据领域的应用

第 8 章 区块链在医疗领域的应用

第 9 章 区块链在教育领域的应用

第 10 章 区块链在公证领域的应用

Block chain

第1章
区块链起源

区块链（Blockchain）的本质是一个不依赖第三方、通过自身分布式节点进行数据存储、验证、传递和交流的网络技术方案，正如一个开放的去中心化的分布式记账本，任何人在任何时候都可以采用相同的技术标准生成信息、延伸区块链。当然，大家要想对区块链有深入了解，必须先要知道区块链的起源。

practice

1.1 区块链的发源——比特币

说到区块链，就不得不提比特币（BitCoin）。比特币诞生于2008年，这时还没有人关注区块链。直到2013年人们才意识到比特币在没有任何中心化机构运营和管理的情况下，依然稳定地运行了将近10年，并且没有出现任何问题。于是，很多人开始注意到比特币的底层技术，即区块链。本节主要介绍区块链与比特币的关系。

1.1.1 数字货币的龙头老大——比特币

数字货币包括数字金币和密码货币，这里只讨论密码货币的范畴。密码货币是一种依靠密码技术和教研技术来创建、分发和维持的数字货币，包括比特币、莱特币、维卡币等。其中，比特币是密码货币之首。

事实上，密码货币的历史很悠久，下面来回顾一下密码货币的发展历史。

1982年，大卫·乔姆（David Chaum）最早提出了不可追踪的密码学网络支付系统，该系统允许一个人发送一串数字到另一个人，而且这个数字可被接收方修改。对加密货币的兴趣以及荷兰历史上对私密性狂热的态度在很大程度上促使大卫·乔姆迁移到荷兰。20世纪80年代末期，荷兰成了密码学和数学研究的温床，而大卫·乔姆也创立了DigiCash，并继续构建依托互联网的加密货币的研究。

尽管大卫·乔姆的研究引起了媒体前所未有的关注，但最后不幸的是，大卫·乔姆和他的公司出现了一些失误，违反了荷兰中央银行的规定。而大卫·乔姆作为妥协，不得不同意公司研发的产品卖给银行。这个调整，给DigiCash公

司带来一个好的预期——试图通过多家银行来创立一个可行的数字现金领域，但最终在 1998 年破产。

在 DigiCash 引起巨大轰动之后，越来越多的创业者试图在这个领域开创一番成就。1998 年，Wei Dai 发表文章称产生了一种匿名的、分布式的电子现金系统，命名为“b-money”。同一时期内，尼克·萨博（Nick Szabo）也发明了“Bit gold”。Bit gold 与比特币的机制非常相似，用户利用竞争解决“工作量证明问题”，然后通过加密算法将解答的结果串联在一起公开发布，从而构成了一个产权认证系统。

Bit gold 是人们公认的“比特币的前身”。随后，哈尔·芬尼（Hal Finney）在 Bit gold 的基础上开发了“可重复利用的工作量证明”。

以上发生的种种引领大家来到了 2008 年。2008 年，“bitcoin.org”域名被悄悄地匿名注册成功。同年 10 月 31 日，一个自称“中本聪”（Satoshi Nakamoto）的人在密码学网站上发表了名为《比特币：一种点对点的电子货币系统》的论文。10 天之后，开源社区 sourceforge.net 上出现了一个叫 bitcoin 的项目。而世界上首批 50 个比特币诞生于 2009 年年初。

中本聪在搭建完比特币体系后似乎就从互联网上彻底消失了，没有人见过他的真正面目。此后，比特币项目由两个前谷歌工程师维护，但即便是这两个人也声称从未见过中本聪。

2010 年，bitcointalk 论坛上用户之间的自发交易产生了比特币的第一个公允汇率。该交易是一名程序员用 10 000 个比特币购买了一个比萨饼。2011 年，维基解密、自由网、Singularity Institute、互联网档案馆、自由软件基金会以及另外一些组织都开始接受比特币的捐赠。2012 年 10 月，全球比特币付款服务提供商 BitPay 发布报告显示，超过 1 000 家商户通过他们的支付系统来接受比特币的付款。

2012 年 11 月，WordPress 博客平台宣布接受比特币付款，还声称比特币可以帮助肯尼亚、海地和古巴等遭受国际支付系统封锁地区的互联网用户购买服务。2013 年 4 月，海盗湾中文网、EZTV 美剧片源网开始接受比特币捐款。同月，中国四川省遭遇雅安地震，公募基金壹基金宣布接受比特币作为地震捐款。

……

截至2017年，比特币已经在全球范围内流行开来。随后，在比特币的带领下，各种密码货币都纷纷崭露头角，走入人们的生活。

1.1.2 从“币”到“链”的颠覆

比特币自诞生之后就陆陆续续吸引了世界各个国家的注意。有了比特币之后，只要有网络就可以完成P2P（个人对个人）交易，不需要借助银行或者其他第三方中介平台。对于投资人来说，比特币就像黄金一样无惧通货膨胀，具有投资价值。

在比特币快速发展的这几年里，与比特币有关的信息一直是人们关注的焦点。比如，比特币价格的涨跌、某快餐店开始接受比特币支付、恐怖分子使用比特币交易、哪个国家政府承认比特币的合法地位，哪个国家反对比特币等。

之后，比特币的发展让其底层技术——区块链——受到了前所未有的关注。人们这才意识到，原来驱动比特币的真正有价值的核心技术是区块链。如果说，比特币对金融秩序的颠覆意义还不够，那么区块链则完全有可能颠覆这个世界。

Chain公司开发了一个以区块链技术为基础的资产交易平台，该平台可以用于市场上任意类型的资产交易，比如货币交易、股票交易、债券交易等；Counterparty、NXT和BitShares基于区块链技术打造的去中心化交易所可以在脱离传统股票交易所的情况下完成股票发行和交易；Guardtime正在研究基于区块链技术的工业级网络安全方面的应用；Holbertson利用区块链技术验证学生的学历，防止学生有学历欺诈行为；Visa和DocuSign致力于通过区块链技术构建汽车租赁市场新商业模式……

未来，如果这些区块链应用全部成为现实并且普遍运用，那么区块链一定会颠覆我们的世界。到时候，如果美国还想试图通过金融封锁的手段制裁一个国家，那么其难度之大可以想象。

区块链之所以具有颠覆意义，是因为它具有以下四个特征，如图1-1所示。

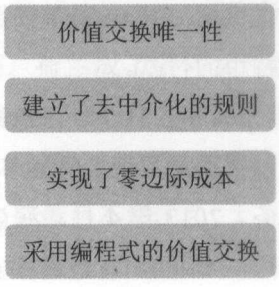


图1-1 区块链的四大特征

第一个特征是价值交换唯一性。价值交换唯一性解决了互联网 P2P 价值交换时出现的信息传递问题。我们在网上发邮件，发给一个人与发给 100 个人，不会出现明显的成本增加。而通过互联网付款时，我们就只能付给一个人。可见，信息可以无限地复制，但价值交换却需要保持其唯一性。而区块链就能保证价值交换的唯一性。

第二个特征是建立了去中介化的规则。这一规则使得互联网在价值交换中实现了去中介化，在没有第三方平台做担保的情况下，即可用双方都信任的算法保证交易。

第三个特征是实现了零边际成本。因为没有第三方参与，只是通过一个算法使双方建立信任关系，所以这里交易的成本就特别低，基本可以实现交易零成本。

第四个特征是采用编程式的价值交换。假如我们通过基金会做一次捐款，用途是修建学校，那么就可以用区块链数字货币去支付这笔钱。即在区块链上写一个小小的程序，把学校的账户写上去，一起寄给基金会。如果基金会不往指定的学校账户支付这笔钱，那这笔钱基金会永远得不到，也汇不出去。在这里，我们支付的不只是钱，还有一段代码。

以比特币为首的所有基于区块链技术的密码货币都只是区块链技术的第一个重量级应用而已。以区块链技术为基础，已经有越来越多的应用出现在我们的视野里，而它们正在颠覆我们的世界。大家不妨跟笔者一起静待区块链时代的到来。

1.1.3　区块链与比特币没有极客说得那么复杂

关于比特币，有种非常夸张的说法是“人类已知金钱的终结”。事实上，很多人对比特币的认知还处于云里雾里的状态。普华永道事务所的消费者调查数据显示，对于比特币熟悉或者非常熟悉的人只有 6%，而 83% 的被调查者表示他们对比特币非常陌生。

与此形成对照的是，“比特币”这一名词的搜索量非常高。以百度指数为例，2017 年 1 月 5 日，“比特币”的用户搜索量达到 80 274 这一峰值。进入 2017 年以来，“比特币”的搜索指数变化曲线如图 1-2 所示。

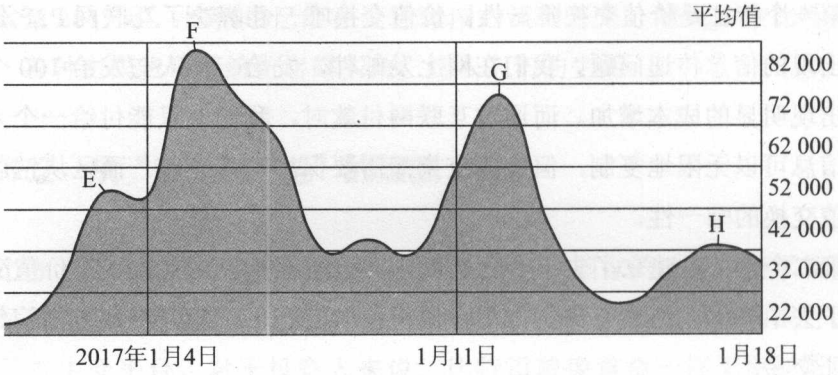


图 1-2 “比特币”的搜索指数变化曲线

那么，比特币到底是什么呢？比特币的本质是一种货币，如果你手上有比特币，就可以按照各外汇市场的汇率用比特币购买商品。也就是说，这和我们用人民币网购以美元标价的产品是一样的。

既然比特币这样简单，为什么大家还是对比特币感到茫然呢？这是因为大部分非技术出身的人认为比特币背后的底层技术区块链是极其复杂的。所以，解释区块链的运作原理是推广比特币的重点和难点。在此之前，几乎没有人会在意银行是如何处理一笔交易的，人们关心的只是账户中的具体交易记录。但是，比特币作为一种未被广泛接受的新事物就必须把一切解释清楚。

众所周知，一本账本必须具有唯一确定性的内容，否则就会有真假之分，从而失去参考意义。所以，记账天然成为一种中心化行为。在技术落后，通信联系不发达的时代，这是必然的选择。在如今的信息时代，中心化的记账方式依然覆盖了社会生活的方方面面。然而，中心化的记账却有一些软肋：一旦这个中心出现问题，如被篡改或者被损坏，整个系统就会面临危机乃至崩溃。另外，整个货币体系作为一个账本系统，也会面临中心控制者滥发导致通货膨胀的风险。

所以说，中心化的记账方式考验中心控制者的能力、参与者对中心者的信任度以及相应的监管法律和手段。那么，有没有可能建立一个不依赖中心以及第三方，但是却可靠的记账系统呢？

区块链解决了这一难题。在互联网信息时代，计算机负责记账，而在记账系统中接入的每一台计算机都是一个“节点”。区块链就是以每个节点的算力

（计算能力）来竞争记账权的一种机制。

在区块链系统中，算力竞赛每十分钟进行一次，每次竞赛的胜利者可获得一次记账的权力，即向区块链这个总账本写入一个新区块的权力。这就导致在一段时间内只有竞争的胜利者才能完成一轮记账，并向其他节点同步增加新的账本信息、产生新的区块。算力竞赛就像购买彩票一样，算力越高就相当于购买的彩票越多，中奖概率越大。

那么，算力竞赛是如何进行的，判定竞赛结果的又是谁呢？区块链的“工作量证明”在这一过程中发挥着重要作用。正如我们早上离开时让保姆打扫房间，晚上回来发现房间一尘不染，尽管我们没有看见保姆工作的过程，但可以确定这些工作已经完成。这就是工作量证明的简单理解，即利用一个人人都能够验证的特定结果确认竞赛参与者完成了相应的工作量。

当然，赢得算力竞赛是有奖励的，即获得比特币。如果没有比特币，节点就没有进行竞争的动力。算力竞赛的奖励也是比特币发行的过程。这种设计是相当精巧的，它将货币的发行与竞争记账机制完美结合到一起，在引入竞争的同时也解决了去中心化货币系统中发行的难题。圈内人士将参与算力竞争试图获得比特币的行为称为“挖矿”。

作为一个记账系统，区块链不仅可以记录以比特币为首的密码货币，还可以记录所有能用数字定义的其他任何资产。

如果你还不明白比特币与你有何关系，那么你只需要知道比特币是另外一种形式的钱就行了。

1.1.4　给你一台计算机，你也可以创造比特币

比特币如此神奇，很多人都想知道除了直接用钱购买之外，还有没有其他方法可以获得比特币？答案是肯定的。比特币存在于互联网数字空间中，隐藏在特定算法里，所以只要利用联网的计算机就能挖掘出来。大家口中所说的“挖矿”就是通过计算机设备运算挖掘比特币，那些专门通过“挖矿”寻找比特币的人就是比特币矿工。

从表面上看，“挖矿”是一个非常简单的过程，只需要利用计算机下载比

特币挖矿工具，然后让设备持续运行就能得到比特币，然后确定账户信息取得对比特币的拥有权。但是，比特币在设计之初已经制定好了规则，产生新比特币的算法难度会随着比特币产生速度的变化而变化。也就是说，矿工挖掘比特币的速度越快，算法难度就会越大；反之，难度越小。

根据比特币挖矿原理可知，计算机的运算能力是挖掘比特币的关键。对于大多数矿工来说，只要打开挖矿客户端，然后挂机就可以坐等比特币的产生。目前，常用的“挖矿”工具有 Ufasoft Coin、Guiminer 等。由于越来越多的人涌入“挖矿”行列中，比特币的产生也随着算力的增大而变得缓慢。下面是影响挖矿收益的四大因素，内容如图 1-3 所示。

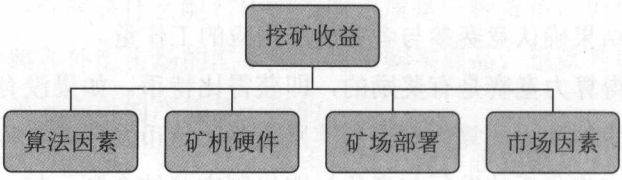


图 1-3　影响挖矿收益的四大因素

1. 算法因素

算法因素是比特币本身的特性，不会受到外部因素影响，但是会影响外部因素，包括算法难度调整周期、每区块收益等。

2. 矿机硬件

矿机硬件是矿工可以通过人力施加影响，从而提高收益的一个因素。一般来说，硬件因素在短期内几乎没有什么变化，而且可预见性、可操作性较高。例如，矿机速度、功耗、成本等，这些因素主要受上游芯片厂商、矿机组装厂商的影响。

3. 矿场部署

矿场指的是比特币矿工团队集体工作的环境。矿场部署是矿场和旷工可以通过人力施加影响，从而提高收益的另一个因素，同样受到上游芯片厂商、矿

机组装厂商的影响，可预见性较高。矿场部署因素包括矿机部署时间、矿场电费、运行保障能力等。

4. 市场因素

比起其他三大因素，市场因素的可预见性较低，但是对挖矿收益的影响非常大。比如，比特币的价格、全网算力增长率、难度增长率等。比特币的价格在短期内波动较小，但是在中长期内何时会出现暴涨暴跌是难以预测的。全网算力和难度增长率在短期内变化幅度会较大，中长期则是会增长趋势。

在影响挖矿收益的四大因素中，算法因素是比特币自身特性，并制约着其他三种因素；矿机硬件的性能和功耗将随着技术升级不断优化；矿场部署的当前趋势是集中化和规模化，通过总量来降低挖矿成本，提升挖矿收益；市场因素受到宏观大环境影响，风险和机遇同时存在。

1.2 疯狂的区块链比特币

如果你还没有听说过“比特疯”这个互联网词汇，你就 OUT 了。“比特疯”寓意为“疯狂的比特币”。作为网络虚拟资产，每一个比特币的诞生、消费记录都记录在区块链上，绝不可能造假。随着比特币的流行，比特币已经可以在大多数国家兑换成为国家法币。数量有限而且具有极强的稀缺性是比特币与其他虚拟货币最大的区别。

1.2.1 比特币的发行规律

本章 1.1 节已经说过，比特币是与区块链一起被中本聪创造的。比特币的获得依赖于计算机程序计算。如果你有一台配置良好的计算机，并且对计算机程序略知一二，那么你就可以下载一个比特币挖掘软件，这样就能在完成特定

数学程序后获得一定数量的比特币。

比特币的发行有两个明显的特征：首先，与人民币、日元、美元不同，比特币没有固定的发行方，而是通过网络节点计算产生的，只要具备了相应条件，任何人都可以参与制造比特币；其次，比特币的发行是限量限速的，这是因为生产比特币的软件算法计算起来非常困难，而且特解方程组所能得到无限个解中的一组有一定的额度限制，这就决定了比特币不会无限量发行。

现存的比特币数量越多，将来挖掘新币的难度也就越大。截至2016年6月，现存的比特币大约有1 566万个。到2140年左右，比特币的产量将达到其上限——2 100万个，如图1-4所示。

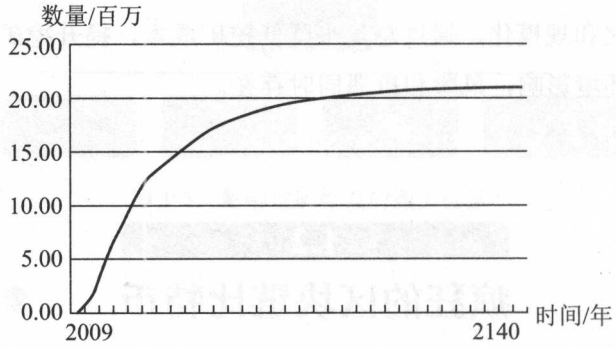


图1-4　区块链比特币数量变化

生产比特币的算法程序通过四年减半的策略控制比特币的发行速度与发行量。也就是说，在比特币刚诞生的2009年1月—2012年1月，约有1 050万个比特币生成。随后的时间里，每四年生产数值就会降低50%。因此，在比特币诞生的第5～9年，生产量为525万个，在第10～13年，生产量为262.5万个，并以此类推。这样，比特币的现存总量永远都不会超过2 100万个，而到2140年的时候，新的比特币几乎就很难找到了。

1.2.2　比特币历史价格变化曲线

试图依靠比特币致富的投资者大有人在，有成功的投资者说：“现在的一枚比特币是一部苹果手机，以后将会成为一栋房子。”据了解，中国是比特币

投资交易最活跃的国家，其次是美国和日本。如图 1-5 所示的是 2009—2016 年比特币在中国日交易量的增长情况。

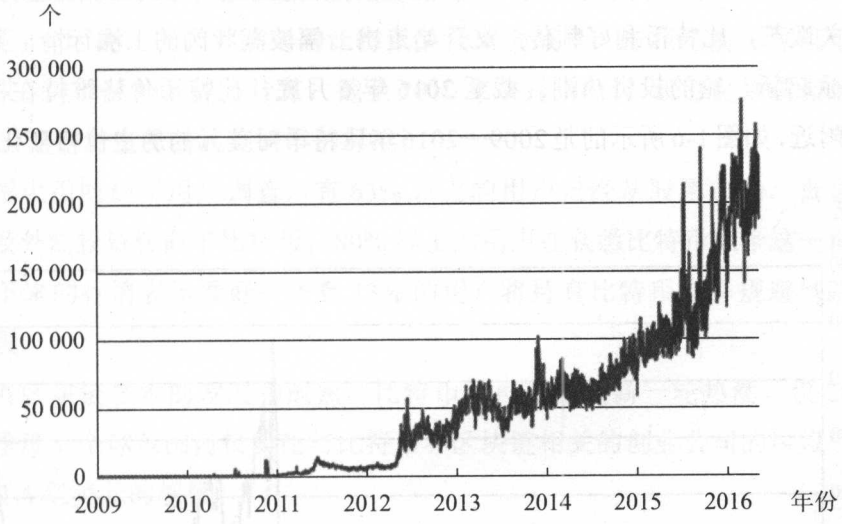


图 1-5　2009—2016 年比特币在中国日交易量的增长情况

在比特币诞生之初，很少有人知道比特币，而且比特币当时没有什么价值。2010 年 5 月 21 日，第一次比特币交易，佛罗里达程序员拉斯洛·豪涅茨（Laszlo Hanyecz）用 1 万比特币购买了价值 25 美元的比萨优惠券。

自 2013 年塞浦路斯发生金融危机后，比特币的价格开始发生巨大变化。某些欧洲国家的法币大幅贬值，而比特币却突然一路高涨，掀起了炒作热潮并带动了整个数字货币行业的掘金狂潮。由于比特币涨价速度过快，拉斯洛·豪涅茨感叹说：“比萨真的很好吃，就是价格有些高。”

2013 年 11 月，比特币攻破 1 000 美元大关，最高时达到 1 200 美元，并一度接近一盎司黄金的价格，综合涨幅超过一万倍，造就了人类历史最大的投资传奇。2014 年之后，比特币市场开始冷静下来，比特币的价值持续降低。

2016 年以来，关于以比特币为代表的数字货币，各国纷纷采取行动。2016 年 1 月 20 日，央行数字货币研讨会在北京召开，并明确表示，央行将争取早日发行央行数字币。与此同时，日本国会也批准有关加密数字货币的新法案，将数字货币视为一种具有货币功能的合法支付形式。另外，作为全球金融

中心之一的英国也宣布发布数字货币 RSCoin 并进行测试。

全球经济大国对去中心化新金融生态的思考，暗含了当前的投资趋势与即将兴起的投资热点。随着各个国家和金融机构相继公布对数字货币的研究进度和相关政策，比特币利好频传，又开始走出一幅波澜壮阔的上涨行情，数字货币也掀起新一轮的投资热潮。截至 2016 年 6 月底，比特币价格维持在 750 美元元附近，如图 1-6 所示的是 2009—2016 年比特币对美元的历史价格变化曲线。

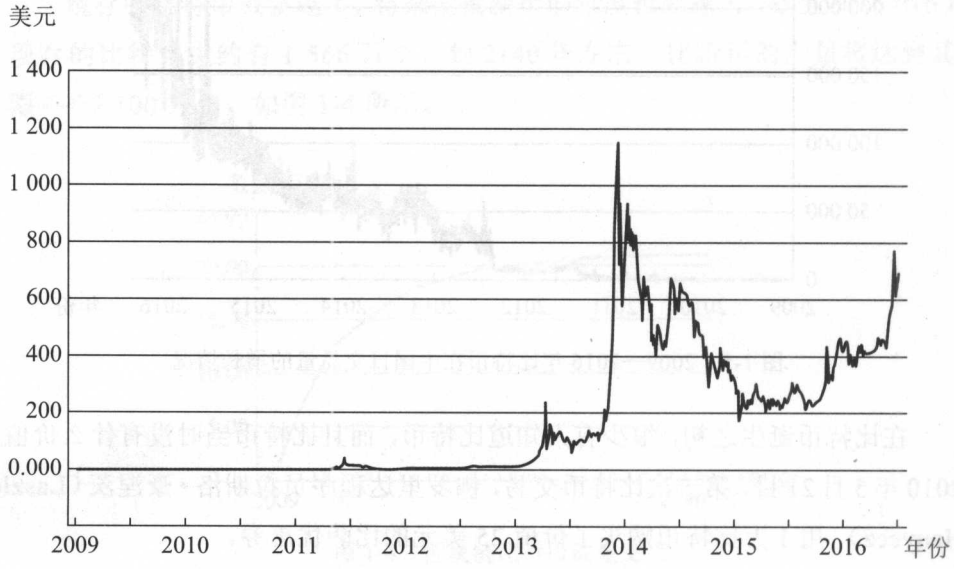


图 1-6　比特币对美元的历史价格变化曲线

看到这里，你是否会感慨比特币的爆发力？

1.2.3　价格一个月涨六成，你见过吗？

2016 年 5 月 18 日—6 月 16 日，这是继 2013 年之后，比特币价格迎来第二个“大牛市”。仅仅一个月的时间，比特币的价格暴涨 61.6%。

根据比特币图表网站（bitcoincharts.com）收集的数据，比特币的交易价格从 452.92 美元飙升至 731.89 美元，交易量从 2 608.23 美元上涨到 6 745 美元，交易总价值从 1 184 326.53 美元上涨到 4 860 262.08 美元。

根据比特币当前的市场价格计算，市场上现存的 1 566 万个比特币的市场

规模约为 109.65 亿美元，约合 731.23 亿人民币。

根据比特币的发行规律，从 2016 年开始，比特币又将迎来下一个产量减半时期，这就是比特币价格暴涨的原因。根据比特币开源软件协议的规定，每生产 21 万个区块，生产者获得的比特币奖励就会减半。按照当前计算机平均每天开采 154 个区块的算力计算，截至 2016 年 7 月 10 日，现存区块就会达到 42 万个，这也就意味着达到减半的标准。

根据火币网最新用户调查，有 63% 以上的用户已经从股票市场、贵金属交易以及外汇投资转向了比特币；80% 以上的用户在获悉比特币减半这一消息后对接下来的行情表示看好；还有 13% 的用户将持有比特币当作规避风险的重要手段。

随着区块链技术的发展和成熟，比特币将再次刮起新一轮热潮。仅 2016 年第一季度，全球范围内投资在与比特币和区块链相关的创业公司的风投资金就达到 1.6 亿美元的规模。

1.3 区块链比特币的价格来自价值，而非投机

投机是股市中的一个概念，即购买的目的是卖。在货币市场中，英镑和日元是投机的典型代表，吸引了大量投机者进行短线操作。与英镑、日元不同，比特币并不是投机品。因为比特币的总量有限，就像黄金一样有保值功能。众所周知，尽管市场中很少使用黄金作为流通货币，但其市值仍然很高，这不只是因为它能够被制成饰品或金属元件，还因为人们更看重黄金的保值功能，因此愿意买入并持有它，比特币的价值原理也是这样。

1.3.1 区块链比特币存储于本地

比特币与虚拟货币有很大的不同，虚拟货币存在于互联网服务器上，而比

特币作为一种字符串，存在于计算机、手机或其他本地硬件设备上。下面一起看比特币与虚拟货币的区别。

虚拟货币是指互联网上非真实的货币，例如，腾讯公司的Q币、Q点、盛大的点券、新浪的微币等。虚拟货币包括网站或应用程序发行的专用货币和游戏币两种。

腾讯公司的Q币就属于网站或应用程序发行的专用货币，可以用来购买QQ会员资格、QQ秀等增值服务，使用比较广泛。与Q币类似的由即时通信工具服务商或门户网站发行的用来购买站内服务的货币都属于这一类虚拟货币。

大多数游戏应用程序都有自己专属的游戏币，而且只能在自身的游戏系统里使用。在游戏里，用户靠打倒敌人、完成签到任务或者直接用钱购买等方式积累游戏币，而用游戏币可购买草药和装备。

比特币是互联网上的数字货币，莱特币、福源币等都属于这种类型的货币。数字货币既可以用于互联网金融投资，也可以作为新式货币用于生活中的某些场景。

如果用户拥有一些比特币的使用权，那么通常需要一个比特币钱包去掌管比特币，例如，PC端的Bitcoin-Qt或者手机端的Bitcoin Wallet。在比特币钱包里，用户会获得一个字符串地址和二维码地址，然后通过这个地址与他人进行比特币交易。

另外，比特币是存储于本地的，所以一旦用户丢失了这个文件，就无法通过网络找到它。然而与实体货币不同的是，比特币是可以备份的，所以用户可以在多个地方保存防止文件丢失。除此以外，用户只要对文件加密，就算别人盗取了比特币文件也难以使用它。

1.3.2 网络是区块链比特币的操控者

网络是比特币的操控者，而不是第三方平台。尽管很多用户出于信任担忧选择利用第三方交易平台进行比特币交易，但交易平台起到的作用只是保证两个地址顺利完成，而比特币的实际流通是匿名而且被整个系统记录下来的。因

此，每个人都可以在 Bitcoin-Qt 这样的比特币钱包里看到任意一笔交易，但是你只能看到一笔比特币从 A 流向了 B，却不知道 A 和 B 分别是谁。

网络操控比特币交易涉及一个重要问题，即怎样避免发生双重支付？双重支付指的是一个人用同一笔比特币同时与两个人发生了交易。在实物货币世界，由于人们无法复制黄金、纸币，所以很容易避免双重支付问题。但是在数字货币世界里，比特币需要通过一个机制去确保比特币所有者无法同时与一个以上的人产生交易行为。

为了解决这个问题，比特币引入了“时间戳”概念。在比特币区块链系统中，每笔交易在通过某个节点或钱包产生时，都需要其他节点验证，即每一个节点都能获知每一笔交易的发生，而且它们有一个公认的交易序列。只有大部分节点都认同这笔交易是首次出现的时候，交易才能发生。也就是说，每一笔比特币交易都盖上了“时间戳”，防止重复支付问题。如果有人重复支付，那么时间就会产生矛盾，系统会自动识别为非法交易。根据一定的利益规则，矿工受利益驱动负责为每一笔交易盖“时间戳”。

矿工的利益是每 10 分钟全网只能竞争到的唯一的合法记账权的奖励。谁竞争到了，就可以获得一定数量比特币的奖励。同时，全网其他矿工要同步一致它这个记账，然后竞争下一个区块记账权。

以计算资源为代价，区块链通过全网作证重新建立了信用体系。一些网友已经开始讨论下一代微信可能是什么，下一个阿里巴巴可能是谁等。事实上，下一个巨头最有可能就是一个真正去中心化的系统。

在未来，如果区块链系统的全网公证为我们作证明，那么数据都是无法作假的。比如，将来我们公证自己和爱人的夫妻关系，这将会在几分钟之内成为全网公开的事实。如果有人想要篡改你们的关系，除非他拥有整个系统超过 50% 的算力，但这几乎是不可能的。

1.3.3　供小于求决定区块链的超高价值

对于在外地工作的人来说，每年春节来临之前都会因为回家的火车票一票难求而苦恼不已。春运被人们戏称为“人类史上最大规模迁徙”。2017 年春

运与往年相比，形势更加严峻。有媒体报道称，2017 年春运有可能成为“史上最难抢票年”。

上述案例表现了一种供小于求的供求关系。当供小于求时，价格上涨，产品的价格是在产品的市场需求和市场供给两种相反力量的相互作用下形成的。产品的均衡价格指的是该产品的市场需求量和市场供给量相等时的价格。与均衡价格水平相对应的供求数量就是均衡数量。

在供给等其他条件不变的情况下，需求变大，均衡价格则上涨，均衡数量同向变动；在需求等其他条件不变的情况下，供给变动分别引起均衡价格的反方向变动和均衡数量的同方向变动。

晶晶是上海一家鲜花店店主，做鲜花生意十几年了。由于情人节临近，大部分鲜花的价格出现了不同程度的上涨。以销量最好的玫瑰花为例，与几天前相比，每扎 20 枝的玫瑰零售价从 150 元涨至 180 ～ 200 元； 每扎 20 枝的康乃馨零售价从 120 元涨至 150 元；百合的价格基本没有变。业内人士分析，情人节前两天，玫瑰花价格上涨还将继续。玫瑰花的均衡价格上涨的原因是其他条件不变，情人节的来临使玫瑰花的市场需求增加。

总而言之，产品的价格与其需求呈正相关，与其供给呈负相关：供给一定，需求增加，则价格上升，需求减少，则价格下降；需求一定，供给增加，则价格下降，供给减少，则价格上升。如果需求和供给同时发生变化，均衡价格和均衡交易量也会发生变化。需求和供给的同时变化，有同方向变化（需求和供给均增加或均减少）和反方向变化（需求增加而供给减少，或需求减少而供给增加）、变动幅度不同（需求的增减大于或小于供给的增减）等情况。

匹配上述所说的供求关系，因为比特币的供给总量一定，但是人们对比特币的需求在日益增大，所以区块链的价格将会越来越高。

Block chain

第2章
区块链——必将颠覆人类世界

大家应当都听说过这种说法，区块链必将颠覆人类世界。现在很多人都很看好区块链的潜力，但是也担心它遭到各国政府捧杀。而且技术创新领域的成功经验也告诉我们，只有消除政府管控、组织和社会等各个方面的障碍，才有可能真正开创区块链革命。如果对区块链占领高地的过程一无所知，就开始区块链创新是不理性的。下面一起看区块链在全球范围内的发展以及各国政府的态度。

practice

2.1

区块链的春天——各国积极表态

比特币受到众人追捧后，各国政府更加关注的是比特币的底层技术区块链。当各国政府逐渐认识到区块链在各个领域的巨大潜力后，有些政府甚至已经开始了区块链的应用计划。下面先看一下各国政府对区块链的积极表态。

2.1.1 中国央行表态支持区块链

2016 年以来，以比特币为代表的数字货币受到各国关注，各国政府纷纷采取行动。2016 年 1 月 20 日，中国央行数字货币研讨会在北京召开，并表示将争取早日发行央行数字币。

中国央行表示，基于区块链技术的数字货币有望实现去中心化结算。而且通过央行的表态可以发现，央行对区块链技术有着客观、深刻的理解，而且肯定了区块链技术比现有的电子货币优势更大。此前，大家担心政府监管部门不会认可区块链，阻碍区块链的推广，此次表态打消了市场疑虑。与此同时，资本市场对区块链的认可度将会进一步提升。

央行前任副行长王永利指出：“数字货币是应用互联网新技术构建全新的货币体系下的货币，这必将对传统的货币发行、货币政策、清算体系、金融体系等产生极其深刻的影响。同时，新的货币体系与传统货币体系、新的金融体系与传统金融体系如何平稳过渡值得关注。”

截至 2017 年 2 月 4 日，中国央行推动的区块链数字票据交易平台已经测试成功。而且央行旗下的数字货币研究所也将在 2017 年上半年正式挂牌成立。这意味着央行将成为全球范围内首个研究数字货币及真实应用的中央银行，并

率先探索了区块链技术在货币发行领域的应用。

那么，央行建立区块链数字票据交易平台对我们的现实生活有什么影响吗？答案是肯定的，大家可以想象一下：不久，过年发红包不再是纸质钞票，而是一串串的数字密码，我们可以通过发送邮件、复制到 U 盘里或者通过手机将红包直接发送给别人。

你或许会问了，这跟用微信、支付宝发红包不一样吗？需要明确的是，数字货币与电子支付方式的感受类似，但是微信、支付宝等电子支付方式交易时所用的钱都是通过银行账户而来，也就是说即便用支付宝、微信交易，我们使用的依然是银行里的钞票。而数字货币本身就是一种具有支付和流通属性的货币，交易时不需要支付宝、微信等第三方中介。

中国央行为什么要开发数字货币？为什么将票据市场作为数字货币的第一个试点应用场景？区块链靠谱吗？如果你心中存在这些疑惑，那么看看央行参事盛松成如何说。

关于中国央行开发数字货币的原因，盛松成称：“区别于已有的电子形式的本位币，安全芯片、移动支付、可信可控云计算、区块链、密码算法等技术是将来数字货币可能涉及的领域。所以，未来的央行数字货币会从多个方面倒逼金融基础设施建设，让我国支付体系进一步完善，支付结算效率进一步提升。更值得一提的是，央行数字货币最后可以构成大数据系统，让经济交易活动的便利性和透明度进一步提高，这将有利于货币政策的有效运行和传导。”

另外，盛松成还总结了央行开发数字货币的四个好处，如图 2-1 所示。

第一	有利于减少洗钱、逃税漏税、逃避资本管制等非法行为
第二	所具有的信息优势使货币指标准确性更高
第三	有利于监管当局进行全面监测和金融风险评估
第四	完善了我国货币政策的利率传导

图 2-1　央行开发数字货币的四个好处

第一，数字货币有利于监管当局追踪资金流向，减少洗钱、逃税漏税、逃避资本管制等非法行为。盛松成表示：“现有的数字货币技术不仅可以记录每笔交易，还可以追踪资金流向。与私人数字货币截然相反，监管当局可以采取

可控匿名机制，掌握央行数字货币使用情况，补充现有的监测控制体系，从而增强现有制度的有效性。”

第二，数字货币所具有的信息优势使货币指标准确性更高。对此，盛松成解释说：“央行数字货币形成的大数据系统，不仅有利于提升货币流通速度的可测量度，还有利于更好地计算货币总量、分析货币结构，这将进一步丰富货币指标体系并提高其准确性。”

第三，数字货币有利于监管当局进行全面监测和金融风险评估。盛松成称：“央行数字货币被全社会普遍接受并使用后，整体的经济活动的透明度会大幅度提高，监管当局可以根据不同的需要收集不同机构、不同频率的完整、实时、真实的交易账簿，这就可以为货币政策和宏观审慎政策提供庞大的数据基础。”

第四，数字货币技术完善了我国货币政策的利率传导。盛松成表示：“只有被全社会广泛认可的央行数字货币才可以把此优势辐射给不同的金融市场参与者，进而提升不同金融市场间的资金流动性和单个金融市场的市场流动性。这将降低整个金融体系的利率水平，使利率期限结构更平滑，货币政策利率传导机制更顺畅。”

综上所述，中国央行开发数字货币的目的不仅仅是取代纸币现金流通，还是适应形势发展、紧跟时代潮流，保留货币主权的控制力，对货币发行和货币政策产生积极的服务作用。

2.1.2 美国政府机构加快布局区块链技术

前美联储主席本·伯南克（Ben Bernanke）曾经表示，比特币以及其他数字货币有可能与现有的在线支付系统一样拥有长期的前途，未来或许可以建立起一个更快的、更安全的以及更有效率的支付系统。另外，本·伯南克也对数字货币表示担忧，认为数字货币有可能带来执法与监管方面的问题。

2013 年 10 月，美国政府关闭了仅使用比特币交易的在线黑市购物网站丝路（Silk Road）。一个月后，美国国土安全和政府事务委员会召开了一次听证会，对捣毁比特币“地下钱庄”丝路一事展开调查。“丝路”事件导致比特币的价格大幅下降，然而美国联邦政府机构（包括美国司法部和财政部等）在对国土

安全和政府事务委员会的致信中称，“比特币在线支付系统所提供的金融服务是合法的”。

美国政府对比特币金融服务的合法表示肯定，表明他们在对待数字货币上的态度由抵制转向了认可与鼓励，这也使比特币价格再创新高。然而在此之前，美国政府一直强调比特币使洗钱以及其他非法活动更加活跃。下面是美国政府 2016 年在区块链领域的布局。

2016 年 4 月，美国国防部先进项目研究局宣布正在研究基于区块链技术的安全信息系统，用于传播加密信息。

2016 年 6 月，美国国土安全部对六家致力于政府区块链应用开发的公司补贴 60 万美元，让企业研究政府的数据分析、连接设备和区块链。

2016 年 7 月 29 日，22 名美国参议员致函美联储要求对区块链进行指导。

2016 年 9 月 12 日，美国众议院通过了一项要求支持区块链技术的无约束力的决议。

2016 年 9 月 14 日，美国众议院议员大卫 • 施卫克特（David Schweikert）提出区块链被视为解决退伍军人事务部管理问题的解决方案。

2016 年 9 月 28 日，美联储主席珍妮特 • 耶伦（Janet Yellen）透露美国央行正在研究区块链技术。

2017 年 1 月 19 日，据火币区块链研究中心编译，区块链成 2017 年度美国联邦贸易委员会金融会议议题。文章称：“近日，美国联邦贸易委员表示，将会在 3 月 9 日举行一次金融科技集会，部分议程将围绕区块链科技及其对于消费者的影响。据周五发布的消息，金融科技论坛（美国商品贸易第三大监管机构）将会就区块链和人工智能为主题展开讨论。该组织在去年连续举办过两场活动，主题集中在众筹和 P2P（点对点）支付。根据美国联邦贸易委员会，该活动将重点关注区块链及人工智能对于消费者的意义，以及两者的影响。”

金融科技论坛在声明中说道：“我们举办这个为期半天的活动目的是聚集行业参与者、消费群、研究人员和政府代表，审视区块链和人工智能在技术发展进步中被应用于为消费者提供服务、潜在利益及消费者保护等方面的意义。”

美国政府机构加快布局区块链将会带动更多国家拥抱区块链，有利于区块链技术在全球范围内的推进和发展。

2.1.3 日本视区块链比特币为现金

2014年6月19日消息称，日本执政党自由民主党（以下简称自民党）表示，暂时不对比特币进行监管。其实，2014年2月25日，全球最大比特币交易平台Mt.Gox正式向法院申请破产保护，估计比特币损失约合4.8亿美元。2015年8月，Mt.Gox的CEO（首席执行官）被捕。日本是第一个遭受巨量比特币损失的国家，此后，日本政府开始考虑比特币监管事宜。

2016年2月29日，日本自民党计划提交认可比特币及其他加密货币货币身份的议案。一旦议案顺利通过，比特币将获得合法的货币地位以及更多的数字货币基础建设投资，同时也将受到更严格的监管并纳税。

日本此项议案是2016年以来首个国家对比特币身份的表态。在此之前，已经有多个国家在2015年对比特币的态度发生了变化。2015年9月，美国商品期货交易委员会（CFTC）正式将比特币纳入大宗商品范围内，并对其进行有序监管。随后，众多不合规的比特币交易平台受到了美国监管机构的制裁。另外，包括英国和瑞士在内的欧洲多个国家等都免除了比特币的增值税。俄罗斯央行也在2015年上半年转变了态度，开始商谈比特币的流通和监管。

2016年5月，日本通过了制定比特币等数字货币规则的资金结算修正案，并将数字货币定义为可用作结算的财产，数字货币与现金进行兑换的交易所将启用登记制度。自此，比特币像现金一样在日本境内流行开来。

日本最大比特币交易所Coincheck的业务发展主管Kagayaki Kawabata表示，资金结算法修正案的实施后将使得比特币成为媒体的新宠儿，推动日本的新趋势。如今，人们已经逐渐改变了旧有的观念，不再仅仅将比特币作为投资工具，而是将比特币用于交易。

截至2017年1月初，在日本大概有5 300个商家及网站支持将比特币作为付款方式，其中99%的商家及网站使用Coincheck付款。与此同时，与2016年1月相比，比特币的月交易金额暴涨了89倍。

在过去，比特币被认为是极客的玩具，但现在它的地位正在发生变化，比特币作为数字货币的合法地位已经被认可。这种观念的转变将会促使越来越多的人使用比特币或其他数字货币进行交易，这也是比特币以及其他数字货币交

易量发生显著增长的主要原因。

Kagayaki Kawabata 对比特币的未来也非常乐观，他认为：“比特币交易量飙升的原因很多，并非偶然事件。尤其是许多大型公司和银行开始对电子货币产生极大的兴趣，并开始尝试区块链技术，预期未来几年电子货币将大幅成长。”

2.1.4　英国央行成公认最“积极”央行

在全球范围内，对区块链技术最感兴趣的央行非英国央行莫属。英国央行对区块链技术的研究与探索非常积极。2016 年 1 月，英国央行发表题为《分布式账本技术：超越区块链》的报告。

报告指出，英国央行正在探索类似于区块链技术的分布式账本技术，并且对区块链技术在传统金融业中的应用潜力进行了全方位分析。另外，英国央行认为，去中心化账本技术重新定义了政府和公民之间的数据共享，在改变公共和私人服务领域有着巨大潜力。

与此同时，英国央行已经建立起一个技术团队专门研究区块链，其行长马克·卡尼（Mark Carney）在 2015 年 9 月也曾表示，正在考虑发行数字货币的可能性。

关于数字货币的研究和技术开发，英国央行一直都在秘密进行中。至于发行国家级数字货币的结果是好是坏，还需要用事实进一步验证。

2016 年，英国央行正式宣布创造数字货币的计划，并将该数字货币称作“RSCoin”。RSCoin 与比特币有很多一样的地方，比如，两者都是使用区块链技术来进行管理的。事实上，区块链对所有的数字货币来说都是必不可少的。

尽管 RSCoin 与比特币的特性相似，但是两者也存在一些区别。其中，最关键的区别是英国央行无法控制比特币的发行与供应，而 RSCoin 的货币供应则是在英国央行内部集中化的。这就意味着英国央行将会创造出 RSCoin 的每个组成部分。这种集中化的货币供应方法要求英国央行必须控制区块链的簿记。

英国央行创造 RSCoin 的目的有两个：一是，通过 RSCoin 使交易活动高效进行，降低交易成本，增大能见度；二是，增强市场信心，并由英国央行对其进行监管，从而降低数字货币带来的不良影响。英国央行之所以有可能对这

种货币进行监管，则是由于区块链技术。

英国央行对数字货币充满了信心，英国央行的一份季度公告表明了其所看重的重点问题。公告称：“数字货币的关键创新在于‘分布式总账’，它允许一种支付系统以一种完全分散化的方式进行运作，不需要银行等中间人。”从这一方面来说，数字货币与当前以电子方式来进行记录的传统货币相差不多。

当前，英国央行将推广 RSCoin，让 RSCoin 在更广泛的范围内得到认可作为主要目标。从这一角度来说，区块链技术的支持是非常重要的。区块链由英国央行控制将会增强使用者对 RSCoin 的信任度。另外，对于以比特币为首的数字货币所面临的数量限制来说，RSCoin 是一种可扩展的解决方案。此前的数字货币在发行总量上受到限制，而 RSCoin 可以随着经济的增长而扩大发行量，这就是 RSCoin 的魅力所在。

比起传统货币，数字货币的货币供应量可以马上受到通货问题的影响，而传统货币的反应较慢。

英国央行积极研究区块链技术，开发数字货币的根本原因在于英国央行试图寻求支付系统的创新，并通过占据区块链技术发展的先机夺回国际金融中心的地位。

另外，银行自动清算业务系统作为英国所有银行进行转账的主要方式，在 2014 年 10 月曾经中断服务长达九个小时。英国银行自动清算业务系统发生的若干次故障也推动了英国央行对区块链技术的探索研究。

无论英国央行积极探索区块链技术的原因是什么，英国央行的行为都对区块链技术在全球范围内的发展起到巨大推动作用。事实上，英国央行已经在某种意义上承认了区块链技术对银行生态系统建设的有利作用。与此同时，我们期待英国央行对区块链的研发取得进一步成果。

2.2 区块链应用的全球进展

在各国政府积极支持的情况下，区块链在全球范围内的发展现状有着非常

良好的氛围，这也使区块链技术越来越被大众所关注。区块链有着非常强大的生命力，正在由外而内地渗透进各行各业。下面一起看区块链应用的全球进展情况。

2.2.1　华尔街各顶级投行对区块链趋之若鹜

高盛集团（Goldman Sachs）是华尔街顶级投行之一，总部在美国纽约。作为世界财富 500 强企业之一，高盛集团的业务范围涵盖投资银行、证券交易和财富管理。高盛在中国香港设有分部，并分别在美国、亚太地区和欧洲 23 个国家和地区设有 41 个办事处。

2016 年年初，高盛发布报告表示，区块链技术已经做好准备要颠覆这个世界。此前，高盛已经和中国 IDG 资本联手向区块链创业公司 Circle Internet Financial 投资 5 000 万美元。

2016 年 5 月底，高盛发布《区块链：将理论应用于实践》报告，展示了区块链将在金融服务、共享经济以及房地产领域如何大显身手。

作为比特币的底层技术，区块链对传统技术的突破在于建立了以 P2P 为基础的去中心化新体系。区块链系统的去中心化使整个网络内的自证明功能成为现实，由中心化的第三方机构进行统一的账簿更新和验证已经成为过去。

行业人士称，比特币是区块链技术的第一个应用，比特币良好的发展状态证明区块链通过去中心化和去信任的方式集体维护一个可靠数据库的方式是可行的。很多华尔街投行都对区块链技术表示相当看好，而高盛只是其中之一。

在长达 88 页的《区块链：将理论应用于实践》报告中，高盛开篇称：“关于区块链技术的讨论，在过去一直都是抽象的，关注的焦点也都是市场去中心化以及去第三方中介的机会，现在我们将关注重点从理论转向实践，研究区块链技术在现实世界中的应用场景。”高盛关注的区块链应用有五个，分别是构建信用体系、实现分布式供电网络、降低房地产交易成本、提高股票交易结算和清算效率、用于客户身份核验。

自 2016 年以来，除了高盛以外，华尔街其他顶级投行也纷纷向区块链技术抛出橄榄枝。前摩根大通高管、信用违约互换（CDS）之母布莱斯·马斯特

斯（Blythe Masters）加入数字货币公司 Digital Asset Holdings，出任 CEO；包括纳斯达克、花旗、Visa 在内的金融行业大咖也向区块链领域大把砸钱，它们联合投资了一家区块链初创公司 Chain，涉及金额高达 3 000 万美元；花旗、摩根大通等顶级投行还向区块链初创公司 Digital Asset 投资 5 000 万美元。

2016 年 1 月，由 10 多家国外大型银行组成的区块链联盟 R3 CEV 对外宣称已经成功实现了区块链技术，在模拟现实（VR）环境下，区块链技术已经初步实现了银行和银行之间的即时交易。未来金融行业的操作标准很有可能就此诞生。区块链联盟 R3 CEV 成员包括花旗银行、富国银行、汇丰银行、瑞士信贷银行等国际著名银行。

华尔街投行们为何对区块链技术趋之若鹜呢？通过数据分析可知，2016 年第一季度，华尔街投行们的 FICC（固定收益证券、货币及商品期货）主营业务收入总额为 178 亿美元，比 2015 第一季度的 248 亿美元下滑了 28.23%。而对比过去五年，这一主营业务的收入总额更是下滑了 49%。

很明显，华尔街投行们正经历着主业萎缩的艰难时刻。主营业务萎缩带来的负面影响就是必须通过大规模裁员以缩减成本。从 2015 年第一季度到 2016 年第一季度，华尔街投行们的 FICC 部门已经从 19 200 人降至 18 300 人，幅度达 5%；在过去 5 年里，FICC 部门总共裁减了 32% 的员工。

在这种情况下，华尔街投行们都试图通过区块链新技术带来的机遇进行自我拯救。

截至 2016 年，高盛、摩根大通、花旗银行、纳斯达克、瑞银集团、桑坦德银行、巴克莱银行、德勤会计师事务所等都成立了区块链实验室，布局这一领域。区块链技术的应用实验已在证券、银行、审计等行业陆续展开。

瑞银集团区块链技术实验室的 PeterStephens 称：“瑞银集团在区块链上已试验了 20 多项金融应用，包括金融交易、支付结算和发行智能债券等。”瑞银的第一个实验是基于区块链技术的智能债券，接下来，瑞银将在积分卡项目推进区块链应用实验。

德勤亚太区投资管理行业合伙人秦谊表示：“区块链技术解决了审计行业历来在满足公众要求、满足监管部门要求方面的难点，能够保证所有财政数据的完整性、永久性和不可更改性，帮助审计师实现实时审计，提高审计效率。”

另外，纳斯达克已经在私人市场启动了区块链技术在股票市场的应用测试。纳斯达克将会利用区块链技术处理私营公司股票交易的大量非正式系统，比如需要律师手动验证电子表格等。

2.2.2　区块链技术应用前景无限扩张

看一下下面的生活场景：我们乘坐的飞机航班是通过微信公众号预定的，飞机降落后我们使用滴滴出行叫到一辆专车，10 分钟后我们到达在美团上预订好的酒店房间，这里地理位置非常好，就在明天开会会场的附近……这种方便快捷的商务旅行生活已经成为一种常态，只要使用当今众多的标志性移动应用就可以实现，比如去哪儿、滴滴出行、美团等。在移动互联网时代，这些应用几乎如影随形。

我们想象一下 10 年后的 2027 年，区块链技术改变了我们的生活，我们可以立即找到提供各种服务的供应商，交易过程更加快捷，不需要借助任何第三方平台。

在未来世界里，区块链使用户获取所有服务的渠道都处于同一个网络中，就像邮件一样采用 P2P 的方式，从而省去加入第三方平台的烦冗手续。而且这个网络中的信息交互都是通过分布式运算引擎上运行的加密算法自动完成的，不会受到任何个体或组织的控制。

在这种环境下，区块链将各种移动应用背后的复杂机制转变成了更完美的系统，帮助用户预订飞机票、订车、订酒店，顺便为用户提供几首你喜爱的音乐。

P2P 基金会的核心成员以及都柏林圣三一学院的讲师 Rachel O’ Dwyer 表示：“区块链创造了一种可信的数字货币和会计系统使人们不必向美联储这样的集中式媒介求助。”

非营利公共信托组织 XDI.org 的网络主席菲尔·温德利（Phil Windley）认为：“区块链非常复杂，这是因为人们希望通过区块链技术解决的问题也很复杂。回想一下 20 世纪 80 年代的光景，当时的人们如果想要给一些计算机建立局域网的话，面临的互联网协议也是异常复杂的。当然，与区块链相比，那些协议还是更简单一些，但是在当时的技术背景下，那就与区块链一般复杂。”

对于区块链技术应用普及的时代，菲尔·温德利非常期待：“区块链能够让我们把所有事物都纳入系统，而不需要任何一家公司作为中间人。当然，公司不会因此全部消失，但是有了区块链技术的应用以后，用户就可以随意更改提供商，所有的服务都能互用。代码全部都是开源的，没有任何一个特殊的组织可以独占某些资源。有了区块链以后，我们甚至有能力运营自己的服务器。”

关于区块链的发展与应用，普遍的说法是将其划分为区块链1.0、区块链2.0和区块链3.0三个阶段。区块链1.0是指以比特币为代表的数字货币应用时代；区块链2.0是指区块链技术在股份、债权、版权、产权等金融领域的扩展应用；区块链3.0是指区块链应用扩展到金融行业之外的司法、医疗、物流等各个领域，全面覆盖人类社会生活，实现信息共享，而不再依靠第三方获得或建立信用。

目前，我国对区块链技术的应用尚处于探索阶段，还没有真正应用起来。但随着相关资源的投入越来越大，一些新型的区块链技术公司正在快速成长，不断地促进各行各业的快速发展，让区块链技术的应用初露锋芒。

2.3 2017年最热门的5家区块链初创公司

在2015年年底，比特币区块链受到了众人的质疑。因此，2016年对比特币来说是至关重要的一年。在比特币没有被广泛认可的情况下，有5家区块链初创公司大力开展比特币业务，开发比特币相关应用程序项目。对比特币的未来发展产生了巨大影响，成为2017年最热门的5家区块链初创公司。

2.3.1 “隐形的比特币公司”——Blockstream

Blockstream是由在比特币领域内做出过重要贡献的比特币爱好者成立的，他们试图通过“侧链”机制来扩展比特币区块链的能力，将比特币的区块链技术应用到包括数字货币、开放资产和智能合约在内的其他资产类型。

2014 年 11 月 18 日，Blockstream 正式宣布获得 2 100 万美元的种子轮融资，资金将会用于探索侧链机制上。

Blockstream 官网的公告显示，此轮融资的投资人分别是 LinkedIn 联合创始人雷德·霍夫曼（Reid Hoffman）、曾投资比特币 API 开发者 Chain 的科斯拉风险投资公司、加拿大种子基金 Real Ventures 等共计 40 位投资者。

Blockstream 的 CEO 奥斯汀·希尔（Austin Hill）表示，Blockstream 之所以能够成功融资是因为高新技术产业逐渐认识到比特币区块链的巨大潜力。奥斯汀·希尔称："Blockstream 是行业内首家致力于扩大比特币协议层功能的公司。也就是说，公司着眼于侧链的扩展机制，使各种创新在一个开放、可互操作的平台上发生。"

在行业里，Blockstream 算得上是资金最充足的创业公司之一，然而 Blockstream 却自称是"隐形的比特币公司"。

有了充足的发展资金后，Blockstream 开始在后台忙碌，并在 2015 年推出了横幅侧链项目的测试版，并公布了首个商业化产品 Liquid。Liquid 的推出将会缩短比特币交易所之间的资金传输时间。

Blockstream 研究开发的另一个项目是闪电网络（Lightning Network），即分布式小额支付网络。这种去中心化的系统可以将小额的比特币交易从区块链移除，此做法不仅加快了交易的速度，还降低了发生费用。另外，闪电网络依然实现了当前比特币网络无须依赖第三方信任的特性。

闪电网络将会降低比特币区块链的交易承载负担，从而使它们无法影响比特币区块的总大小。然而这一项目正面临着一些挑战，比如整合比特币核心。一旦这些问题得到解决，当前的区块大小争论将得到缓解，并且增强比特币网络的健壮性。

2016 年 2 月 3 日，Blockstream 对外宣布获得 A 轮融资，募集资金总额为 5 500 万美元。亚洲富豪李嘉诚旗下维港投资、全球保险集团安盛旗下的 AXA Strategic Ventures 以及日本科技公司 Digital Garage 领投了此轮融资。其他投资者还包括由雅虎创始人杨致远创办的 AME Cloud Ventures、Blockchain Capital 等公司。加上 2014 年的 2 100 万美元种子资金，Blockstream 通过两轮融资中共获得 7 600 万美元的资金。

Blockstream 为什么能受到投资人青睐呢？下面一起看投资人是如何看待 Blockstream 的。

领投方维港投资的公司代表 Fraces Kang 认为：“区块链技术重新定义了金融科技内外的生态系统，释放出无限可能。此次投资 Blockstream 意味着我们将会亲眼见证创新的侧链技术诞生，对此，我们感到非常兴奋。”

AXA Strategic Ventures 管理合伙人 Francois Robinet 则说：“区块链技术不但为金融服务带来变革，也会颠覆其他行业。Blockstream 拥有业内最优秀的技术团队，其开放原始码的做法以及所掌握的侧链技术是我们看重的价值所在。这将会使不同区块链之间进行相互操作，提供关键的长期成效，未来有可能会为保险及资产管理业务带来突破。”

AXA Strategic Ventures 的合作伙伴 Manish Agarwal 认为，公共区块链的商业化是未来大势。Manish Agarwal 表示：“我们相信区块链技术具有重塑金融服务环境的巨大潜力，而公共区块链是最关键的部分。我们对比特币这种数字货币感兴趣，而技术是其关键。”

日本科技公司 Digital Garage 的首席传媒官 Rocky Eda 称：“Linux 系统占据了操作系统的半壁江山，我认为区块链也会故事重演，开源社区将会经过多次测试。”

Rocky Eda 还指出：“日本公司经常把侧链技术用在发展奖励点设计或智能合约之类的应用。侧链是区块链技术的应用开发中最好的解决方案，而私有区块链则显得专有而封闭。”

Manish Agarwal 进一步指出：“侧链的价值地位与比特币区块链的本意较为接近，这种特性更能吸引关注区块链技术的投资公司。我相信这种技术中的价值在于它无须信任的特性，我认为开源证明是其中的关键。”

奥斯汀·希尔也赞同上述观点，他在一篇博客中写道：“这一轮的融资会为 Blockstream 提供资源，继续打造一个开源的结构，这种结构可能会为全球动态信任打下基础。”

结合当前大部分区块链公司都主张抛弃比特币区块链另起炉灶的形势，Blockstream 此次拿到 5 500 万美元的 A 轮融资令比特币技术开发者看到了希望。当前的区块链技术发展还处于探索阶段，面临着各种技术路线的选择。Blockstream 代表着通过比特币区块链以及其侧链来突破限制，实现更多功能。

总体来说，比特币区块链依然是当前最为安全的区块链，而通过开发侧链可以增强平台的开放性，有利于发掘比特币区块链的更大潜力。

2.3.2　在线零售巨头Overstock创造的区块链交易平台——TØ

2015 年 8 月，美国在线零售商 Overstock 的 CEO 帕特里克·伯恩（Patrick Byrne）在美国纳斯达克纽约总部揭露了神秘的区块链交易平台项目 TØ。据悉，Overstock 在 2014 年首次公布了基于区块链的私有和公有股权交易平台。

帕特里克·伯恩解释了的 TØ 的新目标：“我们建立 TØ 平台，在上面交易就是结算，这是一个具有颠覆性的事情。另外，账目的交易和结算也是一体的，它不需要成为各自独立的进程。”

2016 年 4 月，TØ 首次尝试利用区块链技术开启线上股票交易模式。在 Overstock 使用区块链发行私有债券后，TØ 得到美国证券交易委员会（SEC）的批准，发行了公共债券。

下面一起看看票据清算模式的发展史。在纳斯达克证券交易所还没有成立之前，人们为了完成票据的清算，只能骑着自行车，驮着装满债券的包在华尔街上来回奔波。20 世纪 60 年代，美国资本市场经过大规模爆发性增长后迎来了一场危机，骑自行车清算票据的办法已经不能满足当时的市场需求。为了让清算速度赶上交易量，华尔街曾经每周只交易四天，而且每天只有 4 个小时。

1971 年，美国证券交易委员会（sec）召开会议商议如何通过计算机解决票据清算问题。最后，他们讨论出两个方向：一是建立中央对手方（central counterparty）的清算模式，即有一个清算中心，所有交易都要从这里经过，从清算中心系统内展开，经纪人全部要接入这个系统；二是在经纪人之间建立点对点的清算模式，纳斯达克证券交易所的成立就是在这一背景下。

对此，帕特里克·拜恩（patrick byrne）解释说：“第一个解决方向就好像用计算机来安排调度骑自行车的人一样，虽然使用了计算机，但是仍旧没有解决根本问题。”而第二个解决方向被美国证券交易委员会极力推崇，也成为华尔街直到现在依然采用的模式。

帕特里克·拜恩指出：“真正的清算模式应该将交易和清算两个步骤合二

为一同时完成，而不是现在的净额清算（net settlement）。尽管一些金融巨头和硅谷科技公司都在开发应用于市场交易的区块链技术，但是要清楚他们在做什么，只需要问一个问题：清算方式是怎样的？如果他们做的仍旧是净额清算，那么他们就是‘在给骑自行车的人打工’。”

一旦真正的区块链去中心化清算模式取代了现在的中心化清算模式，华尔街某些赚钱的不法勾当将难以进行下去。比如“无货沽空”（naked short selling，也叫“裸卖空”），也就是说在交易市场上出售或者声称出售实际并不持有的资产，以实现在未来以较低的价格买入等额资产的目的。

无货沽空对市场交易有着巨大影响，比如德国曾经在2010年宣布暂时禁止对10家德国银行和保险公司的股票进行无货沽空，从而导致股市大跌。另外，股票借贷（stock loan）、提前交易（front-running）等最赚钱的生意都不再可能。

如果区块链使票据清算模式实现了真正去中心化，那么华尔街将不仅会失去“信息不对称”为其带来的优势，也会失去相应的赚钱能力。可以想象，一旦真正去中心化的清算模式在全球交易市场大规模推广，那些依靠华尔街生存的人就不得不另谋出路。

作为比特币区块链在金融票据领域的应用，TØ平台将会打破多少传统金融服务，只有时间才能给我们答案，大家拭目以待。

2.3.3 比特币消费类应用程序——OpenBazaar

OpenBazzar是一个运用比特币作技术支撑的比特币消费类应用程序。就像是去中心化的eBay（线上拍卖及购物网站），OpenBazaar利用应用程序市场将买家和卖家联系起来，同时用比特币作为交易媒介替代PayPal和信用卡。2016年年底，OpenBazzar继获得100万美元种子资金后，又获得300万美元的A轮融资。

OpenBazaar的诞生加速了比特币向分散市场的发展。一旦该应用取得成功，OpenBazaar将会因为大幅降低各方费用而成为eBay的开源竞争对手。

当前的环境下，电子商务离不开中心化服务。以亚马逊、eBay和其他电商巨头为例，它们对平台上的卖家实施严格监管，并通过收取一定费用盈利。

而且这些公司只接受信用卡和 PayPal 等类似的支付方式，这些支付方式对买家和卖家都收取一定比例的手续费。

另外，这些公司将会获得用户的个人信息。用户面临着信息被盗取或者被卖给他人的风险。在交易过程中，政府和电商公司负责审查所有的交易商品和服务，因此买家和卖家无法做到自由交易。

OpenBazaa 为电子商务带来了另外一种途径，一种让用户掌握权力的途径。OpenBazaar 消除了中心化第三方的角色，将卖家和买家直接联系在一起。由于交易中没有第三方，所以双方都无须支付交易费用。在交易过程中，没有第三方监管，用户可以自主决定是否公开个人信息。

比如，用户 A 想要将使用一年的 iPad5 出售。他首先需要下载 OpenBazaar 客户端，然后在计算机上创建一个产品目录，并标明 iPad5 产品的细节。当用户 A 公布 iPad5 产品的目录后，该目录被发送到 OpenBazaar 的分布式 P2P 网络上。当用户 B 搜索的关键词符合用户 A 设置的“电子产品”“iPad”等关键词时，用户 B 就可以发现用户 A 的商品目录。如果用户 B 不同意用户 A 的报价，可以提出新的报价。

如果两人都同意价格，OpenBazaar 客户端就会使用用户 A 和用户 B 的数字签名为两人创建一个合约，然后将这一合约发送给第三方公证人。如果用户 A 和用户 B 在交易中发生纠纷，公证人就会介入交易。这些公证人和仲裁者与用户 A 和用户 B 一样都是 OpenBazaar 用户。他们既可能是用户 A 的邻居，也可能是用户 B 的朋友，还有可能只是一个陌生人。第三方公证人需要为合约做证，并创建多重签名比特币账户。一旦集齐三个签名中的两个，比特币就会被发送给用户 A。

在这一过程中，用户 B 发送与用户 A 商量好数量的比特币到多重签名地址。用户 A 得到即时通知，确定用户 B 已经发送货款后，就会发出出售的 iPad5，并告诉用户 B 已经发货。几天后，用户 B 收到 iPad5，就会告诉用户 A 已经收到产品，并从多重签名地址释放货款。用户 A 获得了比特币，用户 B 买到了想要的 iPad5，双方都无须支付交易费用，也没有第三方监管交易，用户 A 和用户 B 都得到了想要的结果。

交易中发生纠纷怎么解决呢？与任何网购一样，OpenBazaar 上的交易并

不能保证顺利进行。比如，卖家发错货、没有发货或者产品质量不如预期的好，那该怎么办呢？这时，第三方公证人会介入。只有集齐三把私钥中的两把，才能从多重签名地址中取走货款。而第三方公证人掌握着第三把私钥，所以只要买卖双方没有达成和解或者在第三方公证人判定一方正确之前，多重签名地址中的货款就无法被移动。

那么，如何保证用户对第三方公证人的信任呢？OpenBazaar 设置有一个信誉评分系统，全部用户都有权利对其他用户进行反馈评分。如果一些用户试图交易欺诈，他们的信誉将会受损。如果第三方公证人裁定交易纠纷不够公正，其信誉也会受损。

当用户在 OpenBazaar 平台上购买商品以及选择第三方公证人时，可以通过对方的信誉评分判断他们是否值得信任。当然，OpenBazaar 客户端会通过技术保证评分是合理的，有效防止作弊。具体的步骤非常复杂，但是 OpenBazaar 会处理好这些细节问题。

2016 年 4 月，OpenBazaar 平台正式上线营业，发布了首个完整版本软件并提供下载服务。尽管第一个版本的功能不够丰富，但是该项目充分完成了 18 个月的初期发展，这使数字货币领域为之振奋。

随着完整版本的上线，OpenBazaar 项目负责人表示：“交易本该是免费的。这个想法启发了我们，于是我们花费了两年时间来建设 OpenBazaar 这个平台。从今天开始，世界上任何人，只要能访问互联网，就能使用比特币和 OpenBazaar 来免费交易商品和服务。我们已经迫不及待地想看看大家会如何使用这个工具了。”

2.3.4 搭载比特币的社会化媒体平台——Zapchain

Zapchain 是一个搭载比特币的社会化媒体平台，也是备受期待的区块链初创公司之一。Zapchain 做的是整合链上（on-chain）的比特币微打赏方式，通过革命性的创意促使用户参与高品质的内容创作。

Zapchain 面临的最大挑战在于是否具有可持续发展的能力以及如何避免垃圾用户。据当前的 Zapchain 来说，其避免垃圾用户，遏制垃圾内容的行为已

经出现成效，而且 Zapchain 的用户增长说明其流行度越来越高。

2015 年 11 月 7 日，ZapChain 对外宣布获得 35 万美元的天使轮融资，并公布了与比特币公司（Coinbase）的合作关系，同时推出一个新的数字商品计划。

此轮融资的投资者包括德丰杰（Draper Fisher Jurvetson）合伙人蒂姆·德雷珀（Tim Draper）、Boost VC 创始人兼 CEO 亚当·德雷珀（Adam Draper）以及 Boost 比特币基金。

ZapChain 的首席运营官 Dan Cawrey 表示，这笔资金将被用于平台推广，扩大内容创建者和数字社区成员的范围。

对于投资 ZapChain 的原因，蒂姆·德雷珀解释说："我投资 ZapChain 是因为该公司是最好的比特币应用之一。ZapChain 使得区块链被用于小额支付，为记者和其他媒体人员带来便利，减少与银行之间的摩擦。"

亚当·德雷珀（Adam Draper）也非常看好 ZapChain，他描绘了 ZapChain 内容货币化愿景背后的大画面。亚当·德雷珀是这样说的："微交易很可能是网络内容创作者赚钱的新方式，它可能会改变游戏规则。"

与比特币公司展开合作后，用户可以通过 ZapChain 购买和销售比特币，促进 ZapChain 的数字商品销售。音乐家 Talib Kweli 便尝试了利用 ZapChain 销售他的最新专辑《Indie 500》及单曲。

Talib Kweli 在声明中表示："比特币背后的技术将会帮助人们更容易地获取音乐，并且为音乐家们打开新的市场。" Talib Kweli 还说："做喜欢的音乐并把它带到喜欢它的人面前是一件非常好的事情，不管你在哪里或者你是谁。"

ZapChain 还推出了新的数字社区创新工具微打赏，进一步尝试内容货币化实验。现在，你会发现 ZapChain 平台上的提问和评论旁有一个绿色的"打赏按钮"。如果你觉得某个用户提出的问题或者提供的答案很好，你就可以通过点击此按钮，向其打赏相应数量的比特币，比如价值一个苹果、一杯咖啡、一个比萨饼的比特币。打赏的数额都是平台预先设定好的，用户可以选择但不可以自由设置。

ZapChain 表示，他们并不追求通过该工具获得盈利，他们只希望将该产品推广至其他平台。在 Zapchain 的努力下，Zapchain 终将成为公认的顶级比

特币媒体平台。

2.3.5 资金最充裕的比特币挖矿公司——BitFury

2011 年，瓦列里·瓦维洛夫（Valery Vavilov）和瓦列里·讷班斯尼（Valery Nebesny）共同创建了 BitFury 比特币挖矿公司。由于比特币挖矿的利润不断下降，BitFury 已经将核心角色转变为行业的交易处理器。BitFury 网站上称："整个比特币生态系统都是我们的客户。"

BitFury 堪称资金最充裕的比特币挖矿公司。2014 年 5 月 30 日，Bitfury 正式宣布他们获得 2 000 万美元融资。该融资也是比特币领域最大的融资之一。参与此轮融资的投资者包括 Binary Financial、Crypto Currency Partners、Georgian Co-Investment Fund （GCF）、Queensbridge Venture Partners 和 ZAD 投资公司。

BitFury 的创始人兼 CEO 瓦列里·瓦维洛夫说："这一轮融资的成功表明我们的战略是正确的，让我们有机会向目标迈进——成为世界上第一家公开上市的比特币公司。投资将会大大加速我们的成长，会进一步巩固我们的产品和服务在行业内的领先地位。"

2014 年 10 月 10 日，BitFury 宣布获得新一轮融资，融资金额为 2 000 万美元。此轮融资距离上一轮融资还不到五个月。

2015 年 7 月 10 日，BitFury 宣布完成第三轮 2 000 万美元融资。至此，BitFury 的融资总额达到 6 000 万美元，是竞争对手 KnCMiner 2 900 万美元融资总额的两倍，并占据比特币挖矿行业 1.165 亿美元投资总额的一半以上。

在拿到第三轮融资后，瓦列里·瓦维洛夫（Valery Vavilov）表示："新一轮融资的成功，证明了我们的业务战略，并且令我们更接近我们的宏伟目标。"

第三轮融资的投资方包括格鲁吉亚联合投资基金（The Georgian Co-Investment Fund）、DRW Venture Capital 以及 iTech Capital 等。

DRW Venture Capital 的创始人唐·威尔逊（Don Wilson）对 BitFury 表示了赞赏，他说："我们投资 BitFury，是因为瓦列里·瓦维洛夫的工作令人印象深刻，而且，他们的团队已经成为确保区块链安全业务的行业领导者。"

作为资金最充裕的比特币挖掘公司，BitFury 在 2015 年 12 月 16 日宣布它将在 2016 年第一季度在市场上推出新的 ASIC 芯片。

拿到第三轮融资后，BitFury 宣布将投资 1 亿美元在格鲁吉亚建立一个 100 兆瓦的比特币挖矿数据中心，并推出了 28 纳米比特币挖矿芯片。这是继哥里的第一个 20 兆瓦的数据中心之后 BitFury 在欧亚国家建立的第二个比特币挖矿数据中心。据悉，该数据中心将建在格鲁吉亚首都第比利斯，这里将创建一个特殊的技术区，以吸引国际技术公司。

BitFury 在格鲁吉亚的官方代表 Eprem Urumashvili 表示："格鲁吉亚的受益点表现在三个方面，一是一笔高达 1 亿美元的投资；二是将现代信息技术带入该国；三是格鲁吉亚将因此加入创新技术世界地图。"

值得一提的是，专注于投资格鲁吉亚地区的战略投资基金公司格鲁吉亚联合投资基金连续参与了 BitFury 的三轮 2 000 万美元融资。

2016 年 6 月，BitFury 联合加拿大 NDI 科技公司推出了区块链试行应用——区块链信任加速器（Blockchain Trust Accelerator）。这一应用的意义在于可以连接政府、科技人员和资源来改善治理问题。对于民主制度来说，身份信息、选票以及社会服务等资产都可以被区块链安全且永久地保存。

区块链对加强民主问责制的重大意义已经引起世界各国的关注和重视。比如，区块链信任加速器项目的试行已经于 2016 年 4 月在格鲁吉亚共和国推出。而且，格鲁吉亚共和国政府正在和 BitFury 集团合作创建一种基于区块链的土地所有权数据库。

2016 年 5 月，中国领先的综合互联网金融服务供应商中国信贷控股有限公司宣布与 BitFury 签订协议，用 3 000 万美元购买 BitFury 约 6.38% 的股权。投资完成后，中国信贷将会与 BitFury 在中国成立合营公司销售 BitFury 集团的比特币采矿设备。此次合作对于推广区块链技术，发展以区块链为基础的互联网金融业务有重大意义。

Block chain

第3章
区块链四大核心技术

区块链之所以为大家带来了一个突破传统、颠覆性创新的机会，主要依赖于四大核心技术创新，分别是分布式账本、非对称加密和授权技术、共识机制和智能合约。下面我们分别讲解这四大核心技术。

practice

3.1
分布式账本

区块链使用的记账方式与传统的记账方式不同，具有去中心化创新、数据高度透明、无须依赖信任以及信息可回溯性四大特征。在区块链交易记账操作过程中，分布在不同地方的众多网络节点共同负责记录完整的账本，每一个节点都参与并监督交易的合法性，同时共同为其他用户作证。这种分布式账本的记账方式避免了传统单一记账人因不可控因素而记假账的可能性，保证了账目数据的真实性和安全性。

3.1.1 去中心化创新

区块链的分布式账本是一个去中心化的、没有更高权威的、分布在众多人计算机中的系统。从区块链的本质来说，区块链提供了一种分布式手段来担保和核实交易，从而为最终甩开中心控制者提供了机会。

在传统的交易支付流程中，存在一个中心机构，所有的节点要参与交易必须通过中心机构来达成交易。这里的中心机构既扮演了维护者的身份，维护交易账目正常达成交且真实可靠的，又扮演了特权参与者的身份，发行货币资产的权利。

在区块链的交易流程中，分布式账本的节点 A 直接将交易发给节点 B，所有节点一起确认并且验证交易的真实性。更新了公共总账以后，所有人再同步一下最新的总账。在这里，维护者的身份下放至每一个参与者手中。分布式账本无须对账，大家只需要维护一条总账就可以，这里的总账指的是每个人都可以看到公共账簿。

分布式账本去中心化的特点为区块链未来发展奠定了应用基础，下面以区块链技术在跨境电商领域的应用为例，介绍这一特征。

跨境电商是从2016年火起来的。随着国家政策层面的扶持加强，跨境电商成为新的行业风口。根据行业预测，2017年中国跨境电商交易额将达到8万亿元，年均增速超过30%。

当前，我国跨境电商存在一些问题。首先是外贸渠道的缺失和信任问题。外贸大环境非常复杂，对商家的要求也非常高，而国内品牌商的外贸之路因为外贸渠道缺失和信任问题而显得迷雾重重。

其次是手续费高昂和转账周期长的问题。以传统跨境汇款方式电汇为例，汇款周期一般长达3～5个工作日，这期间除了中间银行会收取一定手续费，环球银行金融电信协会（SWIFT）也会对通过其系统进行的电文交换收取较高的电信费。在我国通过中国银行进行跨境汇款时，单笔汇款的电信费为150元。

订单碎片化也是跨境电商面临的一大挑战。在全球金融危机后，中国外贸发生显著变化，短期订单、中小订单逐渐代替长期订单、大订单。可以说，市场体量庞大，订单碎片化已成为外贸新常态。

在线贸易的刚性需求及交易频次提高的同时利润下降，这是跨境电商面临的另一个挑战。在这种情况下，外贸制造商必须全面转型，从简单的生产制造商进化为贸易综合服务商，以适应全球市场的竞争。

支付不仅是供应链系统的引擎，也是跨境电商的重要环节，其支付模式直接决定跨境电商的生命线。我国国内的第三方支付系统比较发达，但是在国外就不一样了。为了解决跨境电商发展中的难题，关于区块链支付的讨论应运而生。可以说，区块链支付为跨境电商提供了近乎完美的支付解决方案。

区块链分布式账本的去中心化创新使用户在跨境汇款中以更低的费用和更快的速度完成跨境转账，市场空间非常大。

传统的跨境支付方式具有清算时间长、手续费高、容易出现支付诈骗行为的劣势，跨境资金风险较大。区块链打造的P2P支付具有去中心化的特征，不但可以全天候支付、瞬间到账，还能降低隐形成本，有利于降低跨境电商资金风险及满足跨境电商对支付清算服务的便捷性需求。

下面我们一起看一下区块链支付为跨境电商提供的解决方案。区块链分布

式账本构成一个去中心的全球结汇系统。这个系统的核心机制包括两方面内容。

一是引入网关系统，解决陌生人之间转账汇款的信任问题。一般来说，银行、第三方机构等具有公信力的主体都可以担任网关。用户与网关之间的关系在整个系统中反映为一种债权债务关系，即如果用户 A 需要通过区块链钱包汇款给用户 B，则其间的网关就与 A 生成了债务，与 B 生成了债权，通过将该网关对 B 的债权转为 A 对 B 的债权并进行清算，继而反映在双方余额变化上就完成了交易。

A 与 B 之间的债权债务关系利用区块链的分布式账本储存在若干个服务器上，而服务器之间以 P2P 的方式进行通信，以避免中心化服务器所带来的各种风险。

二是根据共识选择用于结算的数字货币，如比特币、莱特币等。数字货币的作用是维护系统正常运行，防止恶意攻击者大量制造垃圾账目蓄意破坏。因此区块链钱包要求每个网关都必须持有一定限额的数字货币量，并且每进行一次交易，都需要提供一定量的数字货币，就像传统的每次交易都要交手续费一样。

在区块链打造的跨境结算方式中，银行也可以参与进来。银行不需要提供技术支持和底层协议，只要指定特定的数字货币履行这一职责就可以了。这种模式将会代替传统成本高昂的 SWIFT 技术，从而帮助传统银行以更低的成本、更快的速度来进行跨境清算和汇款。当然银行还可以选择覆盖更多的支付场景和数字币种，就像淘宝和京东为用户提供多样的结算方式一样。

基于分布式账本技术，区块链将会帮助跨境支付解决现存问题，增强跨境电商参与方的体验。

3.1.2 数据高度透明

2016 年 7 月 30 日，支付宝爱心捐赠平台上线了一个新项目，名为“听障儿童重获新声”。该项目将会筹集 19.84 万元善款，用于听障儿童一年的听力语言康复、聋健融合教育和人工耳蜗调机费用。这一项目与往常的爱心项目有什么不同呢？细心的捐赠人可以发现，在反馈页面查看善款去向时增加了“爱心传递记录”。

这表明该项目的资金募集及使用将受到公众全程监督，善款在何时流向哪个账户是一目了然的。用户首次可以亲眼见证自己的捐款从支付宝平台划拨到项目执行方账号，最终进入受助人指定账号。这一改变不仅是视觉和用户体验上的升级，更是蚂蚁金服首次尝试将区块链技术应用于公益场景。

对于规模较小、实力薄弱的公益机构来说，提升透明度、打造公信力是非常困难的。举例来说，捐款人捐5元后索要免税发票，而项目方邮寄发票就需要15元，而且这还没有计算项目方投入的时间和精力成本。在这种情况下，将区块链用于公益显得非常有价值。

蚂蚁金服首席技术官程立称："在支付宝爱心捐赠平台上，经常有用户捐出几元到几百元不等的善款，但捐款离开公益项目的支付宝账户后，就很难再被用户追踪。而区块链公益平台就像一家专门邮寄善款的互联网邮局。每笔善款都是一个包裹，在投递过程中，经过每个邮寄节点都会被盖上邮戳，每个邮戳都可以被公开查询。"

中华社会救助基金会秘书长胡广华认为，区块链的分布式账本数据高度透明的属性将打造一种不需要第三方背书的新信任机制。他说："区块链技术让支付宝平台、公益机构支付宝账户、受助人支付宝账户无缝链接起来，成为一个可追溯的闭环，这是低成本高效率，专业公益、有效公益的重要尝试，对提升公益透明度和信任度是一次革命性的助推。"

蚂蚁金服表示，他们将会在合法合规、保证用户信息和资金安全的前提下，与更多的公益组织和审计机构展开合作，让区块链技术助力中国公益信任环境的改善。

将区块链用于公益主要借助了分布式账本数据高度透明，从而达到提升公众信任度的作用。区块链分布式账本向所有的参与者公开数据，让大家共享一个账簿，并通过去中心化的管理达到人人平等，这些创意是前所未有的，并且因此受到广泛关注。

区块链分布式账本的数据对所有的人公开，所有的参与者都能在互联网上共享这些数据，保证了账本的公正性。而且比特币、以太坊超级账簿以及大部分的竞争币系统都具有这种特征。它们对所有人都公开，表明人人都能通过一台联网计算机进入。

以比特币为例，所有的参与者 ID 都是匿名的，但是上面的数据默认对所有人都公开。这种开放性带来了巨大的优势，比如抵抗专制制度资本管控以及抵抗攻击的能力。比特币在保证对所有人公开的同时还具有安全的特征。我们甚至无法想象，只要我们愿意，就能够获知每一个参与者的账户余额以及交易记录。

直到现在，人们依然惊奇于比特币保障安全的方法是如此的新颖，而且在它存在的近 10 年历史中，竟然从来没有人切实可行地打破过这种安全。与之相对，如果用最传统的方法保护用户权利和安全，那么风险是非常高的。这种模式的雏形开始于世界第一把锁的发明。一把锁一般只有几把钥匙，这会让所有者觉得安心。然而，很多例子都证明这种模式失败的可能性很大，钥匙可以被设计得很聪明，但总有聪明的盗窃者不用钥匙就可以打开这把锁。

如果一位用户在计算机的数据库里保存着一些公司的绝密数据，那么一场黑客竞赛也就开始了，胜利者将会以很小的成本获得这些数据，威胁公司的安全。但区块链就不一样了，比特币经过众多考验之后依然保证安全则说明了这一点。显而易见的是，黑客对于比特币在网络中每天潜在交割的 67 亿美元的价值毫无下手的机会。

有人说，区块链比特币可以用于贩卖毒品以及其他违禁类产品和服务。这是事实，但用 1 万美元也能做这些事情，任何纸币都可以。如果说，人们可以接受纸币的匿名性，那为什么要抗拒区块链比特币呢？

事实上，区块链比特币虽然具有匿名性，但是比特币区块链上发生的交易很容易就能进行追踪，任何人都可以查询，而纸币的使用则无迹可寻。业内人士曾经尝试过根据序列号追踪纸币使用踪迹的研究，但是几年后被证明是不可行的。下面是比特币对比纸币的三大优势，如图 3-1 所示。

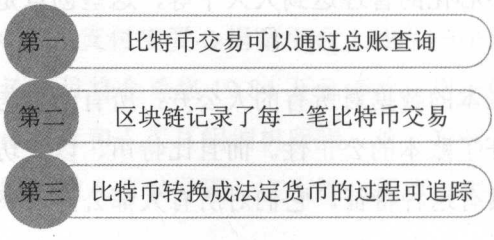


图 3-1　比特币对比纸币的三大优势

第一，比特币交易可以通过总账查询。如今，纸币的追踪依赖于实物检查的方式，而区块链比特币的优势则更明显。区块链比特币的本质是一个庞大的分布式账本，每一笔网络交易都由节点记录在系统中，尽管交易双方钱包的所有者是匿名的，但总账是公开的。包括执法机关、税务当局在内的所有机构和个人都可以访问总账。

第二，区块链记录了每一笔比特币交易。区块链记录了系统中发生的每一笔交易，因此我们可以在总账中查询到所有的交易历史。每一笔比特币交易都可以查询，无法隐藏、改变或者篡改，远远好于纸币消失又出现，交易或转移的情况无迹可寻。如果没有记录，纸币交易各方的情况是无法查询的，而比特币交易则会显示在总账里，除了比特币钱包所有者的身份信息。

第三，比特币转换成法定货币的过程可追踪。另外，比特币对法定货币的转换过程也是可以被追踪的，因为用户要想将持有的比特币转换为法定货币，必须与交易所或提供类似服务的机构进行联系。所有提供相关服务的交易所以及机构都处于相关部门的监管下，以帮助执法机构对犯罪行为进行追踪。

相比之下，纸币可以无限循环使用，无须转换成其他形态。对于罪犯来说，使用比特币的犯罪行为更容易被执法机构追踪到，所以他们更愿意选择真正匿名的纸币。

3.1.3　无须依赖信任的哈希算法

哈希算法也被称为“散列”，是区块链的四大核心技术之一。由于一段数据只有一个哈希值，所以哈希算法可以用于检验数据的完整性。在快速查找和加密算法的应用方面，哈希算法的使用非常普遍。

在互联网时代，尽管人与人之间的距离更近了，但是信任问题却更严重了。现存的第三方中介组织的技术架构都是私密而且中心化的，这种模式永远都无法从根本上解决互信以及价值转移的问题。因此，区块链技术将会利用去中心化的数据库架构完成数据交互信任背书，实现全球互信的一大跨步。在这一过程中，哈希算法发挥了重要作用。

可以说，以比特币为首的数字货币并非区块链最重要的价值体现，在信息

不对称、环境未知的情况下建立一个满足人们经济活动需求的信任生态体系才是区块链更重要的意义。

下面我们一起看一下区块链是如何通过哈希算法解决信任问题的。在此之前，我们需要解释一下什么是“拜占庭将军问题”。

“拜占庭将军问题”是由著名计算机科学家莱斯利·兰伯特（Leslie Lamport）提出的点对点通信中的基本问题，也可称为“两军问题”或者“拜占庭容错”。

在5～15世纪，拜占庭就是当时的东罗马帝国，也就是现在土耳其的伊斯坦布尔。可以想象，拜占庭军队有许多分支，驻守在敌人城外随时准备进攻，每一个分支都有各自的将军。当时的环境决定了骑马传递信息是将军之间通信和协调统计进攻时间的唯一途径。

由于敌人的防御比较强大，任何一个军队分支的单独入侵行动都会失败，而且入侵的分支还会被歼灭。因此，只有一半以上的分支同时进攻才能成功占领敌人的城池。

在观察了敌情以后，将军们需要制订出一个统一的进攻计划，即确定出在哪一天的哪一时刻进攻。然而将军中存在一个叛徒，他的任务就是破坏忠诚将军们的进攻计划，使他们的进攻不能达成一致。这样只要进攻时的军队分支少于一半，敌人就会胜利，叛徒的目的就达到了。这是一个由互不信任的各方构成的网络，但是他们需要完成一个共同使命（除叛徒以外）。

由于各个将军之间互相不信任，认为只有在自己的城堡以及军队范围内才能保障自己的生命安全，所以将军们不会聚集到一起开会。在这种情况下，他们在任意时间以任意频率派出任意数量的信使到任意对方，内容如下：“我将在第×天的第×点进攻，你同意吗？”

如果收到信息的将军同意该做法，他就会在原信上附上一份盖章验证的回信，然后把合并之后的信息拷贝再次发送给其余的将军们，要求他们也这样做。他们的目标就是通过原始信息的积累使最后的信息链盖上他们所有将军的图章，在时间上达成共识。

问题出现在这里，假设有10个将军，每个将军向其他9个将军派出一名信使，那么就是10个将军每人派出了9名信使，而在任意时间内有总计90次

的传输，并且每个将军分别收到 9 个信息，可能每一封信的进攻时间都不同。另外，叛变的将军还会同意超过一个以上将军的攻击时间，然后重新广播超过一条的信息链。于是，这个系统迅速演变成一个信息虚假和攻击时间相互矛盾的纠结体。

拜占庭将军问题是一个在分布式系统中进行数据交互时面临的难题，也就是说当整个网络中的分布式节点之间都没有信任度，如何操作才能保证信息交互的安全性而且不用担心数据被篡改。区块链利用哈希算法完成了这一挑战，使系统中所有节点在无须信任的条件下自动安全地交换数据。

区块链是这样做的：它为信息发送加入了成本，降低了信息传递的速率，而且加入了一个随机元素使在一段时间内只有一个将军可以广播信息。这里所说的成本就是区块链系统中基于随机哈希算法的“工作量证明”。哈希算法所做的事情就是计算获得的输入数据，得到遗传 64 位的随机数字和字母的字符串。

区块链系统计算的输入数据是指节点发送的当前时间点的整个总账。当前计算机的算力使其可以实时计算出单个哈希值，但是比特币区块链系统只接受前 13 个字符是 0 的哈希值结果作为“工作量证明”。而前 13 个字符是 0 的哈希值是非常罕见的，需要整个比特币网络花费 10 分钟的时间才在数以亿计的数据中找到一个。在一个有效的哈希值被计算出来之前，网络中已经生产了无数个无效值，这就是降低信息传递速率，并使整个系统成功运行的“工作量证明”。

在拜占庭将军问题中，第一个广播信息的将军就是第一个发现有效哈希值的计算机，只要其他将军接收到并验证通过了这个有效哈希值和附着在上面的信息，他们就只能使用新的信息更新他们的总账拷贝，然后重新计算哈希值。下一个计算出有效哈希值的将军就可以将自己再次更新的信息附着在有效哈希值上广播给大家。然后哈希计算竞赛从一个新的开始点重新开始。由于网络信息的持续同步，所有网络上的计算机都使用着同一版本的总账。

比特币区块链系统找到有效哈希值的时间间隔为 10 分钟，这是算法设置好的。算法难度每隔两周调整一次的目的就是保证这 10 分钟的间隔，不能多也不能少。每隔 10 分钟，总账的信息就会在区块链更新并在全网同步一次，因此分散的交易记录是在所有网络上的计算机之间进行对账和同步的。

当用户在区块链系统发起一笔交易的时候，他们会使用私钥和公钥为这笔

交易签名，而内嵌在区块链系统的标准公钥则承担了加密工具的角色，对应在拜占庭将军问题中，加密工具就是用于签名和验证消息的印章。

因此，哈希算法对信息传递速率的限制加上加密工具使区块链构成了一个无须信任的数据交互系统。在区块链上，一系列的交易、时间约定、域名记录、政治投票系统或者任何其他需要建立分布式协议的地方，参与者都可以达成一致。

区块链通过哈希算法解决了拜占庭将军问题，而且这一方案可以推广开来。那些在分布式网络上无法解决信任问题的领域都可以通过区块链得到解决。比如，互联网领域的专家们正在试图为互联网创造一个分布式的域名系统；基于区块链技术的互联网选举投票系统也正在研发中。如果说，互联网云分享搅动了一池春水，那么区块链构建的不依赖信任的交易系统则打开了洪水闸门。

3.1.4 银行也抵抗不了的信息可回溯性

2011 年的郭美美炫富事件直接导致公众对红十字会的信任度下降；2016 年震惊全国的雷洋事件始终真相不清；魏则西事件让我们看到了信息不对称社会下的个体悲剧……

如果有了区块链，一切就不一样了。比如，建立区块链公益，记录每一笔捐款的收入和支出，使信息完全对公众公开。区块链分布式账本的可回溯性使“郭美美”们将无法隐藏；如果规定警方出警的时候必须通过指定的多台设备实时上传到区块链视频云上，那么真相将水落石出；如果建立一个区块链平台记录医院信用以及治疗方法，就可以规避由于被不对称信息和不实广告所蒙蔽而产生的悲剧。

总之，这一切改变基于区块链分布式账本的信息可回溯性。下面以区块链在互联网金融领域的应用为例看信息可回溯性的重要性。

2016 年 6 月，中国互联网金融（青岛）高峰论坛在青岛召开。安存科技旗下公司北京安金网络科技有限公司副总裁马成龙在论坛上做出发言：“互联网金融领域之所以有这么多乱象发生，根源在于在互联网这个虚拟空间里，记录主体行为的载体变成了电子数据，很难追溯。”

关于马成龙口中的电子数据，我国最高法院发布的《关于适用〈中华人民共和国民事诉讼法〉的解释》是这样规定的：“电子数据是指形成于或者存储于电子介质里的信息数据。”在互联网行业，电子数据主要指的是电子协议、电子合同以及电子支付凭证等。

电子数据常常与用户的权益挂钩，因为用户的投资项目、投资时间、投资金额、投资的收益回报等信息都可能是通过电子数据记录的。当用户的权益受损时，这些电子数据将成为用户证明自己权利的最核心资料。

然而，实际操作中会出现很多问题。尽管法律承认电子数据可以充当证据，但是电子数据通常都是由平台单方面保管的。用户与平台方发生利益纠纷的时候，平台方很有可能会将电子数据摧毁或者进行篡改。在这种情况下，用户根本无法使用真正具有效力的电子数据进行维权。

下面看一个P2P理财的例子：一家理财平台曾经将本应向投资者还款的时间全部延迟一年之久。当投资者想要使用电子合同维权时，发现该平台已经私自在网站内修改双方的合同协议内容，并且私自添加了还款协议；另外，各种网贷P2P平台跑路事件也闹得沸沸扬扬。每当平台跑路后，投资人会发现他们的网站、APP已经无法打开，所有的电子数据都消失殆尽。在这种情况下，执法机关调查取证困难，投资人的维权之路非常艰难。

对于这种现象，马成龙表示：“这些鲜明的例子都在警惕互联网金融消费者，提高电子数据保全意识，用法律的武器保护自己是维护自身权益的根本之道。”

近几年来，政府工作报告都提到了互联网金融。2014年的表述是“互联网金融异军突起”，2015年的表述是“促进互联网金融健康发展”，而2016年对互联网金融的表述为“规范发展互联网金融”。由此可见，政府已经把互联网规范放在了第一位。在规范互联网金融发展的过程中，区块链具有非常大的价值。

比如在P2P网贷行业，2015年倒闭跑路的917家P2P网贷平台中，90%以上的平台都设立了资金池，由于内幕操作无法兑付而选择了跑路。由于信息的不对称性，投资者根本无法知道平台是否设立了资金池、资产是真是假以及资金用途，而且更做不到一一考证。因此，只有用上永久存储以及无法篡改数

据的区块链技术，才能保证 P2P 平台仅仅充当信息中介，不触碰资金。毕竟信息的可回溯性让 P2P 平台难以在众人的监督下做出违法勾当。

再比如票据业务领域，2016 年 1 月 22 日，中国农业银行北京分行保险柜中票据换报纸的新闻震惊了全国。当天，中国农业银行正式发布公告称："农行北京分行票据买入返售业务发生重大风险事件，经核查，涉及风险金额为 39.15 亿。本应存放在银行保险柜里的票据，却被某票据中介提前取出，与另外一家银行进行了回购贴现交易，但资金并未回到农行北京分行的账上，而是非法进入股市，又由于近期 A 股下跌，导致巨额资金缺口无法兑付。"

票据业务领域的乱象非常多，除了一票多卖等票据违规交易问题，还包括克隆票、假票、变造票等违规操作问题。在这种情况下，市场急需一种更安全、完善的票据交易模式，而区块链为这种模式提供了可能。

作为一种永久存储，信息不可篡改的分布式账本，区块链由数以亿计的大量计算机节点共同维护。复杂的校验机制使得保存在区块链上的数据具有连续性和一致性，就算某些计算机造假篡改了数据也无法改变整个区块链的完整性。私钥签名和公钥验证交易内容全部正确后，数字货币就会在对应的账户地址间转移，而且保证准确无误。

因此，将区块链技术应用到 P2P 网贷领域以及票据业务领域的电子数据存储上，将会彻底解决许多违法违规的问题。一个投资项目的发起到资金筹集，再到后期的偿还以及一张票据从申请到发行，从交易到承兑，整个流程的关键信息都会记录在区块链上，谁都无法篡改。

基于区块链上信息的可回溯性，监管部门的查询将变得非常容易。另外，数字货币的转移路径明确，这就使 P2P 平台只能将投资者的资金用于规定的用途，最后回到投资者手里。而中国农业银行北京分行的票据即使被暗箱提取贴现交易，资金也只能回到中国农业银行北京分行的账上，第三方无法插手。作为全球最热门的金融科技，我国的互联网金融也需要依靠区块链技术崛起。

客观上信息不对称以及主观上受到利益驱使加大了中心节点产生欺骗和伪造信用的风险。区块链技术的加入可以在时间维度上保证连续性，在空间纬度上保证开放性。总而言之，区块链上信息的可回溯性将会影响众多领域，而这种可回溯性是银行业也难以抗拒的。

3.2
非对称加密和授权技术

区块链中每一个数据块中包含了一次网络交易的信息，产生相关联数据块所使用的技术就是非对称加密技术。非对称加密技术的作用是验证信息的有效性和生成下一个区块。另外，区块链上网络交易的信息是公开透明的，但是用户的身份信息是被高度加密的。只有经过用户授权，区块链才能得到该身份信息，从而保证了数据的安全性和个人信息的隐私性。

3.2.1　私钥掌握在用户手里

由于私钥是非对称加密技术涉及的概念，所以我们首先探讨对称加密技术以及非对称加密技术。对称加密技术的特点是数据加密和解密使用的密钥（意思是秘密的钥匙，在密码学中，密钥是在明文转换为密文或将密文转换为明文的算法中输入的参数）相同。也就是说，加密密钥也被用作解密密钥。这种加密技术在密码学中叫作对称加密技术。

对称加密技术的优势是使用方便，密钥简洁而且破译难度高。DES、3DES、Blowfish、IDEA、RC4、RC5、RC6 和 AES 是较为常见的对称加密技术。

在电子商务交易中，对称加密技术主要存在四个问题，内容如图 3-2 所示。

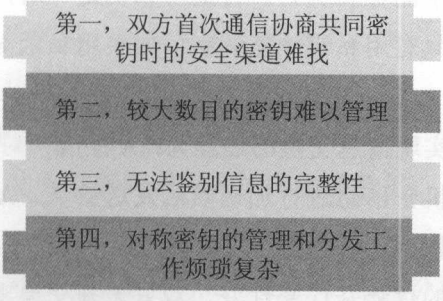


图 3-2　对称加密技术的四个问题

第一，双方首次通信协商共同密钥时的安全渠道难找。直接的面对面协商

是协商共同密钥最安全的方式，但这是不现实而且难以实施的。因此双方很可能会选择其他相对不够安全的渠道进行协商，包括使用 QQ、微信、发送邮件或者通电话等。

第二，较大数目的密钥难以管理。对于一方来说，对于每一个合作者使用的密钥都不相同。在开放的社会环境中存在大量的信息交流，而数目较大的密钥与社会发展环境是难以适应的。

第三，无法鉴别信息的完整性。对称加密技术不具有鉴别信息完整性的功能，因此发送者和接受者的身份也是无法验证的。

第四，对称密钥的管理和分发工作烦琐复杂。采用对称加密技术的贸易双方必须使用相同的密钥，保证密钥的安全可靠。另外，双方还需要设置防止密钥泄密和更改密钥的程序。

如果两个用户使用对称加密技术交换数据，那么涉及的密钥为 2 个。如果企业有 n 个用户，那这个企业共需要密钥的个数为 $n\times(n-1)$ 个。如此看来，企业信息部门需要在密钥生成和分发工作上付出很大一部分精力。

为解决信息公开传送和密钥管理问题，公开密钥系统应运而生。相对于对称加密技术，这种方法也叫作非对称加密算法。非对称加密技术允许通信双方在不安全的媒体上交换信息，安全地达成一致的密钥。RSA、ECC（用于移动设备）、Diffie-Hellman、El Gamal、DSA（用于数字签名）是比较常见的非对称加密技术。

非对称加密技术中存在两个密钥，一个是公开密钥（以下简称公钥），另一个是私有密钥（以下简称私钥）。公钥与私钥是一对，在加密时，如果用公钥对数据加密，那么只有用私钥才能解密；如果用私钥对数据加密，那么只有用公钥才能解密。

非对称加密技术实现信息交换的过程为：A 生成一对密钥，并将公钥公开。B 得到公钥后用其对机密信息进行加密然后发送给 A。A 再用自己保存的私钥对加密后的信息进行解密。

非对称加密技术的优势是保密性好，双方无须交换密钥，缺点是加密和解密花费的时间长、速度慢。

如果企业中有 n 个用户，那么企业需要生成的密钥数目为 n 对，并将 n 个

公钥公开，n 个私钥由用户自己保存。由于用户掌握的私钥是唯一的，其他用户可以通过公钥来验证信息发送者的来源是否真实可靠，而信息发送者也无法否认发送过该信息。

作为区块链的核心技术之一，非对称加密技术可以用于用户的身份验证。由于用户掌握的私钥是唯一的，所以身份验证显得非常容易。下面一起来看中本聪通过比特币的创世块证明自己身份的原理。

比特币的创世块有 50 个比特币，而且代码是确定、唯一的，这就使这 50 个比特币不能使用。中本聪的创世块地址为“1A1zP1eP5QGefi2DMPTfTL5SLmv7DivfNa”，很多比特币爱好者还向中本聪的地址捐币，使其余额超过了 50 比特币。对中本聪来说，他拥有这笔比特币的所有权，但是没有使用权。

比如说，一个比特币的狂热爱好者在网上发言，并称自己就是中本聪本人。如果中本聪自己觉得有必要澄清，就可以使用创世块的私钥签名，并注明该发言并非由自己本人发出，全世界的人们就知道真相了。

那么我们每个人以及企业机构等如何使用区块链来标识自己的身份呢？首先，我们需要使用比特币 QT 钱包（比特币本地钱包）生成一个收款地址，该收款地址可以是空地址，不需要有任何余额。其次，我们需要用 QT 钱包对生成的空地址进行签名。签名一般都是使用特定消息，然后就可以得到签名结果。然后，我们需要向全世界公布自己的比特币地址，包括特定消息和签名结果。这时，全世界都知道了这个地址是我们的。

如果在一些情景下，你需要向对方证明你的身份，那么对方给出一个特定消息，你只需要签名，对方进行验证即可证明你的身份。

用区块链验证身份的唯一风险就是私钥被盗，所以只要用户妥善保管好自己的私钥，别人就无法伪造你的身份。

截至 2017 年年初，区块链数据已经超过了 25G，如果我们仅仅使用 QT 钱包进行身份验证，就不需要同步庞大的区块链数据，否则启动和关闭 QT 钱包都无比慢。

一个企业机构也可以使用这种方法验证自己的身份真假。与个人一样，企业需要使用一个地址进行签名声明自己是该私钥的唯一拥有者。很多时候，企业的身份都是由多人共同确认的，遇到这种情况，企业可以预先将私钥分成多

份，让几个人共同保管。比如私钥分成三份，只有两人以及两人以上共同签名才能确认企业的身份。在这种情况下，企业遇到任何伪造机构身份的行为，都可被轻易验证。

区块链让人类第一次不需要依靠任何第三方中心机构就可以完成身份验证，也是人类第一次在互联网上创造了一个不能复制、不可伪造的数据库。

从比特币创世块开始，世界已经发生改变。也许到2026年，你可能会看到以下场景成为事实。一个英国海关官员对某个中国游客说：“先生，请对这一消息‘welcome to England’，在您的比特币地址‘×××’上签名。”该先生拿出手机，点了点，官员也在他的桌面设备上点了点，然后说：“welcome to England，×××。”

基于非对称加密技术，区块链将如何改变我们的生活呢？只有时间才可以验证。

3.2.2 匿名，这里可以实现

区块链的授权技术保证了未经用户授权，任何人都无法获知用户的身份信息。下面以比特币为例，看用户如何实现合理的匿名性。

试想一下，发送和接受比特币就好比作者用笔名发表作品。如果作者的笔名与自己的身份无关，那么谁都无法得知作品背后的作家的真实身份。在区块链上，用户接收比特币的地址是公开的，凡是与该地址有关的交易信息都会被永久保存在区块链上。如果用户的地址与真实身份没有任何关系，那么用户便实现了合理的匿名性。

要实现匿名，用户需要保证比特币钱包地址与自己的身份信息没有关联。也就是说，用户需要匿名购买比特币。下面是三种匿名购买比特币的方法，内容如图3-3所示。

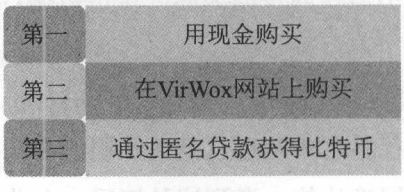


图3-3 三种匿名购买比特币的方法

用现金购买是匿名购买比特币最好的选择。大多数比特币在线交易的过程是类似的，即需要用户上传身份证。而用现金购买可以避免在线交易，不用上传身份证用户，可以亲自接见比特币卖方，支付现金即可获得比特币。只要用户愿意，用现金购买比特币有很多可以使用的方法来避免卖方知道自己的身份信息。

在 VirWox 网站上购买比特币也可以实现一定的匿名性。当然，在 VirWox 上购买比特币无法实现完全匿名，因为该网站仍然要求用户透露一些信息。不过，相比于其他一些比特币在线交易要求用户提供银行账户和个人证件信息，通过 VirWox 网站购买比特币可以实现更好的匿名性。

在 VirWox 网站上，用户需要一个免费账户来购买林登币（第二人生 3D 网络游戏里的虚拟游戏币）。用户可以使用的支付方式有 PayPal、Skrill 等。为了实现更好的匿名性，用户可以选择使用 paysafecard 支付。有了 paysafecard，即便没有身份证、银行账户或者信用卡，用户也可以购买林登币，还可以在无须验证的情况下将林登币兑换成比特币。

通过匿名贷款获得比特币也是一种可行方式。根据以往经验，用信用卡购买比特币是很难实现匿名的。但是，比特币贷款就不一样了。比如，Reddit 就免除了小额贷款项目中复杂的身份认证过程。

事实上，以区块链作为底层技术支持的数字货币都可以实现匿名，下面我们看看新兴数字货币 ZCash 如何实现匿名的。

ZCash 与比特币一样，都建立在区块链之上。不同的是，ZCash 实现了完全的匿名。ZCash 有一个非常特别的功能，即用户可以自由选择隐私级别，自主决定公开哪些数据。比如，一个大学生接受了父母给其发送的一笔 ZCash，然后这个大学生将隐私级别设置为只有父母可以看到这笔钱的交易信息。

ZCash 的发明者以及公司 CEO Zooko Wilcox 称：“这款新型货币使用者的身份将在真正意义上难以识别，使其管理具有更强的保密性。”尽管比特币等数字货币都具有匿名性，但在现实生活中我们可以通过区块链的记录与追踪交易获知比特币的发送地点，从而定位到发送者。

然而 ZCash 通过密码计算，即零知识证明（密码学术语，意思是在不让对方知道任何信息的条件下证明一件事）保证了用户在不泄露身份信息以及执行金额的情况下进行交易，给了用户更多的控制权。

对此，ZCash 官网有如下说明：“不同于比特币，ZCash 的交易完全对发送者、接受者以及交易链中的其他信息保密。只有那些有权限者才能够了解交易细节。使用者有完全的控制权自行决定是否赋予他人了解交易细节的权限。”

ZCash 的设想最早出现在 2014 年 Zooko Wilcox 的一篇学术论文中。按照计划，ZCash 的开发工作非常顺利，并且取得了初步进展。当然，在形成完整的开放系统之前，Zooko Wilcox 还需要做很多工作。

为了进一步调试 ZCash 的开发和设计，ZCash 团队于 2016 年 7 月推出了 Zcash 测试版。同时，人们可以通过 ZCash 网站上“testnet”系统参与测试版的体验，提前使用这种当前没有价值但未来将有很大升值空间的货币。

2016 年 10 月 28 日，ZCash 正式推出同名数字货币—— ZCash。Zooko Wilcox 说：“我们非常兴奋，因为 ZCash 数字货币的诞生意味着区块链属性和加密功能首次结合在了一起。”

比如说，如果用户使用 ZCash 完成了一笔交易，区块链上留下的信息就是交易发生了，而具体花费了几个 ZCash 货币，购买了什么，只有用户自己才知道。

Zooko Wilcox 还说：“ZCash 通过给每笔交易加密，解决了用户的隐私问题。我们使用的加密算法是标准的、现代的、高科技的，如同保护网站、电子邮件和互联网上一切内容的加密方式一样。”

ZCash 的投资人 Roger Ver 说：“经济学规律和物理学规律一样都是一成不变的。优秀的货币应当是每一个单位都与其他任何单位都一样。对于数字货币来说，将其设为私有是最好的方法。”

如果有足够多的人关心数字货币交易的匿名性问题，那么这种货币将会大获成功。其实，早在 1998 年，DigiCash 由于日常消费者对金融隐私不够重视而宣告破产，但随着人们对隐私的重视度增强，DigiCash 的历史应当不会重演。

Zooko Wilcox 对 ZCash 的未来也非常有信心，他说：“我认为隐私具有重要的个人和社会价值，它可以保护个人和社会的隐私，让个人和社会的价值升值。每当有关 ZCash 项目的文章出现的时候，网友或者身边的朋友们就会告诉我他们也感受到了这一点。他们对此非常开心，并且很高兴看到我们为之努力，他们希望我们能够成功。”

无论是比特币还是 ZCash 都说明了一点，区块链可以帮助人们实现匿名，这不仅仅是梦想。

3.3 共识机制

区块链的共识机制用于验证每一次记录的有效性，从而防止任意节点篡改数据。区块链上的共识机制有很多种，不同的应用场景根据效率和安全性的考量选择不同的共识机制。共识机制主要包括工作量证明（Proof of Work，PoW）、权益证明（Proof of Stake，PoS）、股份授权证明（Delegate Proof of Stake，DPoS），其简介如表 3-1 所示。

表 3-1　区块链三种共识机制的简介

共识机制	工作原理	优点	缺点	使用项目
工作量证明	利用机器进行数学运算来竞争记账权；与其他共识机制相比，资源消耗高、可监管性弱；每次达成共识需要全网共同参与运算，性能效率比较低；容错性方面允许全网 50% 节点出错	完全去中心化，节点自由进出	比特币已经吸引全球大部分的算力，其他再用工作量证明机制的区块链应用很难获得相同的算力来保障自身的安全；挖矿造成大量的资源浪费；共识达成的周期较长	比特币；以太坊前三个阶段，即 Frontier（前沿）、Homestead（家园）、Metropolis（大都会）
权益证明	节点记账权的获得难度与节点持有的权益成反比；比工作量证明机制的资源消耗少，性能有所提升，但依然是基于哈希运算竞争获取记账权的方式，可监管性弱；容错性方面允许全网 50% 节点出错；权益证明是工作量证明的升级版本，根据每个节点所占代币的比例和时间等比例的降低挖矿难度，从而加快找随机数的速度	在一定程度上缩短了共识达成的时间；不再需要大量消耗能源挖矿	本质上依然是挖矿，没有解决商业应用的痛点；这种确认是一种概率上的表达，不能保证是一个确定性的事情，理论上有可能存在其他攻击影响。例如，以太坊的 The DAO 攻击事件造成以太坊硬分叉，而 ETC 由此事件出现，事实上证明了此次硬分叉的失败	以太坊第四个阶段，即 Serenity（宁静）

续表

共识机制	工作原理	优点	缺点	使用项目
股权授权证明	与权益证明的主要区别在于节点选举若干代理人，由代理人验证和记账；其合规监管、性能、资源消耗和容错性与权益证明相似。类似于董事会投票，持币者投出一定数量的节点，代理他们进行验证和记账	大幅缩小参与验证和记账节点的数量，可以达到秒级的共识验证	整个共识机制依然依赖于代币，而很多商业应用是不需要代币存在的	点点币（Peercoin）和未来币（NXT）

3.3.1 工作量证明机制

由于比特币是区块链的第一个产物，所以，我们以比特币为例讲述区块链的共识机制——工作量证明。

本书 1.1.3 小节中讲道，比特币区块链是以每个节点的算力来竞争记账权的一个系统。在区块链系统中，算力竞赛每十分钟进行一次，而竞赛的胜利者就获得一次记账的权力，即向区块链这个总账本写入记录的权力。这就导致在一段时间内只有竞争的胜利者才能完成一轮记账并向其他节点同步增加新的账本信息、产生新的区块。

作为一个记账系统，区块链不仅可以记录以比特币为代表的数字形式的货币，还可以记录能用数字定义的其他任何资产。这意味着区块链可以定义更为复杂的交易逻辑，比如股权、产权、债权、版权、合约、公证、投票等可以用数字形式进行价值存储或转移的任何东西。但是，当区块链应用于不同场景时，使用的共识机制就不一定是工作量证明机制了，还有可能是上文提到的权益证明机制、股权授权证明机制或者其他共识机制。

3.3.2 中心维护到参与者共同维护

在区块链共识机制发挥作用的过程中，所有当前参与的节点共同维护着交

易及数据库，它使交易基于密码学原理而不基于信任，使任何达成一致的双方，能够直接进行支付交易，无须第三方参与。

作为记录交易的数据结构，区块链由众多已经达成交易的区块连接在一起形成，所有参与计算的节点都记录了主链或主链的一部分。在区块链上，每一个节点都有一份完整的已有区块链备份记录，而这些都是通过进行数据验证算法解密的矿工网络自动完成的。区块链上保留着所有关于每个节点和节点上比特币余额的信息，这些信息也被记录在完整的区块链上。

公共式区块链账本完全对外公开，这意味着区块链信息可以通过特定地址在区块链浏览器上进行查询。因此，我们才敢肯定地说，区块链通过均等的节点权利和义务保证了绝对公正。

大家可以想象一下以下这个场景：这里有两个银行和两个用户——银行甲和银行乙以及用户A和用户B，用户A还使用一款第三方支付软件丙。银行甲、银行乙以及第三方支付丙都分别用自己的信息系统为用户记录账户余额，这基本上就是当今金融世界里的样子。

在银行甲的系统中有如下记录："银行乙欠自己100万美元；用户A透支了20万元人民币；用户B有存款5万元人民币。"

在银行乙的系统中有如下记录："自己欠银行甲100万美元；用户A有存款12万元人民币；用户B有存款4万元人民币；自己在第三方支付丙上有200万元人民币。"

而用户A在银行甲透支了20万元人民币，在银行乙有存款12万元人民币，在第三方支付丙上还有2万元人民币的余额。因此，只有通过两个银行和一个第三方支付的三个系统才能计算出用户A真正拥有的财产。

我们可以看到，银行甲与银行乙之间100万美元的借款被记录了两次。事实上，每个银行都必须花费大量的时间与金钱去开发和维护系统用来记录信息。更麻烦的是它们需要花费更多的时间和金钱在各银行之间互相检查对账，银行业的数据还需要使用多个不同的系统去记录。而且银行需要在对账方面付出高昂的成本，以确保各方信息的准确性。

下面用一张图表来记录上面例子中的所有数据，如表3-2所示。

表 3-2 银行、用户以及第三方支付之间的所有数据

甲方	乙方	数额	货币类型
银行甲	银行乙	100 万	美元
银行甲	用户 A	20 万	人民币
银行乙	第三方支付丙	200 万	人民币
用户 A	银行乙	12 万	人民币
用户 A	第三方支付丙	2 万	人民币
用户 B	银行甲	5 万	人民币
用户 B	银行乙	4 万	人民币

表 3-2 和之前银行各自记录的内容是一样的，但是这种记录方式使得银行与用户之间不用维护自己的系统，而且最关键的是完全省去了银行之间对账的流程。这时可能有人就会有疑问，为什么不用一个统一账本记账呢？区块链就是这样做的。

区块链是一个共享网络，所有银行和用户都在这个网络当中，没有一个中心系统会维护账本，取而代之的是网络中的所有银行和用户都有这个账本的最新内容，账本由网络中的所有参与者共同维护。这样就防止了中心系统故障引起的账本丢失，而且每个参与者都对账本的安全与稳定起到了重要作用。

3.4 智能合约

智能合约指的是基于区块链中不可被随意篡改的数据自动化执行一些预先设定好的规则和条款，比如基于用户真实的信息数据进行自动理赔的医疗保险。区块链使智能合约有机会用于现实生活中。

3.4.1 以数字形式定义的承诺

智能合约（smart contract）的概念可以追溯到 1995 年，由密码学家和数

字货币研究者尼克·萨博（Nick Szabo）提出。尼克·萨博对智能合约的定义如下：“智能合约是一套以数字形式定义的承诺（promises），合约参与方可以在上面执行这些承诺的协议。”

在该定义中，“一套承诺”指的是合约双方共同制定的权利和义务，合约的本质和目的都将通过这些承诺体现出来。以一个买卖合约为例，一套承诺指的是卖家承诺发送货物，买家承诺支付合理的货款。

“数字形式”指的是合约将会以可读代码的形式写入计算机。因为智能合约建立的权利和义务是通过计算机网络执行的，所以参与方达成协定后必须完成这一步操作。

“协议”指的是合约承诺被实现的技术，合约履行期间被交易资产的本质决定了协议的选择。还是以买卖合约为例，假设买卖双方都同意使用比特币作为支付方式。在这种情况下，双方选择的实现合约承诺的技术就是比特币协议，智能合约将会在比特币协议上实现。在这里，用比特币脚本语言的数字形式定义合约承诺。

智能合约的诞生扩大了区块链的应用范围，更多的指令将会通过区块链智能合约来执行。由于智能合约完全是代码定义和执行的，所以实现了完全自动而且人工无法干预的模式。智能合约的操作方式是由其自治、自足、去中心化的三大特征决定的。

自治指的是智能合约一旦启动就会自动执行整个过程，包括发起人在内的任何人都没有能力进行干预；自足指的是智能合约通过加强服务或者发行资产的方式来获取资金；去中心化指的是智能合约的运行系统是分布式的，没有中心化的服务器，而且通过网络节点自动运行。

尼克·萨博认为，智能合约最简单的形式就是自动售卖机。两者的道理是一样的，用自动售卖机买东西，只要放入钱，选择商品，商品就会自动掉出。操作相同，结果相同。而智能合约只要有预先设定好的代码，就会一直按照代码来执行，代码相同，执行结果相同。

在商业领域，很多问题的执行依赖于信任，这使执行变得非常复杂，而智能合约帮助大家解决了这一难题。当高效的全自动执行系统替代了低效的人工判断机制，智能合约在最小化信任的基础上让事情变得更加便捷。

下面以智能遗嘱为例，看智能合约的应用。假设“如果父亲去世，儿子在结婚后才可以获得其财产”是一个智能遗嘱。这个交易事件需要到未来某个事件发生或者未来某个时间点被触发才能执行合同。第一个条件是父亲去世，系统首先会扫描一份在线死亡数据库证明父亲已经去世；第二个条件是儿子结婚，当智能合约确认了死亡信息后，程序会设定一个交易日期，一旦通过婚姻信息在线数据库扫描到儿子登记结婚，就会自动发送财产到儿子名下。

区块链智能合约在遗嘱执行方面的应用已经被某些公司关注，比如Blockchain Apparatus。Blockchain Apparatus是美国Blockchain Technologies Corp集团启动的众多创业公司之一。该公司致力于研究基于区块链技术的新应用，目前从事一些法律领域方面的研究，这为法律服务行业提供新发展。

截至2016年7月，Blockchain Apparatus已经开发了一些区块链投票创新应用，并且开始研究执行医嘱的区块链智能合约。将遗嘱管理交给软件来运行，无须人为控制，这在历史上第一次有可能实现，而且这一创新应用必将在未来改变人们管理自己财产的方式。

Blockchain Technologies Corp的法律顾问成员艾瑞克·迪克逊（Eric Dixon）认为：“智能遗嘱或者更广泛的智能合约文件击中了大部分家庭和法院诉讼代理人的心。它在一个可定义且固定的时间内为立遗嘱人的真实意愿提供了更有力的证据。”

当前，因为无法保证遗嘱的真实性而导致的遗嘱诉讼案件非常多，遗嘱的表述模棱两可或者无法处理而造成解读分歧，这也是发生遗嘱诉讼案件的原因之一。

艾瑞克·迪克逊强调说：“区块链智能遗嘱可以保证遗嘱的真实性、排除伪造的可能性、使遗嘱的维护变得更容易、使法院获得事实的速度加快。”

区块链技术允许遗嘱修改，每次修改存储在其原始状态，而不需要经过繁杂的法律程序。艾瑞克·迪克逊解释说：“区块链将文件创作和提交到区块链的信息全部记录下来，很容易就能证明遗嘱的存在。这样一来，猜测一份遗嘱签订的时间将是一件愚蠢的事情，因为区块链给出了最好的答案。”

智能遗嘱只是一个开始，智能合约还将会改变政府、企业以及个人管理文件的方式。总而言之，智能合约有着广泛的应用领域，但产业化之路还需要大

家共同探索。

3.4.2　全面解析智能期权合约

期权与股票一样是一种金融工具，是买方向卖方支付一定的权利金后拥有的在未来某一时间段内或特定日期以事先约定价格向卖方购买或出售特定商品的权力，分为看涨期权和看跌期权。

看涨期权指的是在合约规定的有效时间内，期权持有者按照规定价格和数量购进相应标的物的权力。期权持有者之所以购买这种期权，是因为他对标的物的价格看涨，可以在未来获利。与之对应的，看跌期权指的是在合约规定的有效时间内，期权持有者按照规定价格和数量出售相应标的物的权力。

下面我们以看涨期权为例，讲解期权的运作过程。购买看涨期权后，如果标的物的市价高于合约规定的价格与期权费用之和时（不包括佣金），期权持有者就可以按照合约规定的价格和数量购买标的物，然后按照市价出售或者转让买进的期权，获取利润；如果标的物的市价高于合约规定的价格，但是低于合约规定的价格与期权费用之和，那么期权持有者将会损失一部分期权费用；如果标的物市价低于合约规定的价格时，那么期权持有者将会损失全部的期权费用，而且没有行权权力。综上，期权持有者购买期权的最大损失为期权费用加佣金。

比如，一个石油提炼商根据形势判断原油的价格会上涨，于是想到购买原油看涨期权。他以每桶 0.5 美元权利金的价格买入了执行价格为 54 美元 / 桶的 100 手合约（每一手合约代表 1 000 桶原油）。在到期时，该石油提炼商的收益损失如表 3-3 所示。

表 3-3　石油提炼商的收益损失

市场价格（美元 / 桶）	结果
大于 54.5	收益 =（市场价格 − 54.5）×1 000×100
54.5	损益平衡点
54 ～ 54.5	损失 =（54.5 − 市场价格）×1 000×100
小于 54	损失 =0.5×1 000×100（全部权力金）

了解了期权的运作过程后，我们接着看智能合约在期权领域的应用。以一个简单的智能期权合约为例，甲从乙处购买了智能股票期权合约，这个合约就使乙可以用每股 10 元的价格购买甲在 A 公司的 2 000 股股票。这个合约规定了期限，如果乙超过期限未行权，期权合约将自动作废。

智能股票期权合约定义的相关条款包括合约相关资产、合约方身份、行使价、合同有效期等。合约到期以前，智能期权合约的“exercise”功能将会自动执行持有人以行使价购买股份的行为。首先，“exercise”功能会检查发起交易者是否是合约股票的持有人，然后检查当前是否依旧是合约有效期。如果两者检查均通过，合同会立即执行，系统户根据合约条款将现金从持有人一方转移到卖家一方，而将股票资产转移给持有人。

截至 2017 年，智能合约还仅仅作为理论存在着。智能合约应用到现实世界里有两大难题。

第一个难题是智能合约难以把控实物资产保证合约的有效执行。以售货机为例，售货机通过将商品保存在内部硬件中严控财产所有权，但是代码应当怎么做呢？在智能期权合约中，“exercise”功能需要在合约双方之间转移现金和股份资产，但是计算机程序要怎么控制现实世界的现金、股份等资产呢？

第二个难题是智能合约难以获得合约双方的信任。对于合约代码以及解释和执行代码的计算机，合约双方需要有一个共享的标准，可以验证计算机是否有问题。

当前，区块链技术的发展应用还处于探索阶段，但是没有人怀疑区块链将会解决智能合约面临的两大难题。

首先，区块链使得计算机代码控制现实资产，保证智能合约的有效执行。区块链数字货币可以使现实资产转化为计算机代码，从而控制现实中的资产。在区块链上，资产的控制不需要控制实物，而是控制资产对应的密钥。因此，在上述案例中，期权智能合约就可以控制合约相关资产，而不需要代管机构。一旦启动“exercise”功能，代码执行就可以完成资产转移，无须人力参与。

其次，区块链解决了信任难题。区块链的功能不仅限于数据库，还可以记录资产所有权以及执行代码的分布式计算机。期权持有者可以将购买的期权上传并存储在区块链中，并根据指令执行。区块链这一优势同样适用于执行智能合约。一旦区块链记录了合约代码，合约方就可以确定合约不会被更改。

区块链智能合约离我们的生活并不遥远。证券交易所、银行以及其他金融机构都在积极研究开发区块链相关应用，希望可以实现利用区块链技术记录和交易现实资产的功能。

目前，通过区块链技术将智能合约的应用真正落地还处于研究探索期，但是区块链是人类发现的首个可以实现智能合约商业用途的技术。

3.4.3　票据理财的守护神——数字化契约

“收益不需要太高，只要安全；模式新不新不重要，只要能够正常运营”这体现了投资人对理财风险的无奈表态。在股市、基金、P2P、股权众筹纷纷不乐观的情况下，一直以“安全”著称的票据理财也出现了诸多意外。

2016年1月22日，中国农业银行北京分行买入返售业务发生重大风险事件，这一新闻震惊了全国。

当天，中国农业银行正式发布公告称：“农行北京分行票据买入返售业务发生重大风险事件，经核查，涉及风险金额为39.15亿元。本应存放在银行保险柜里的票据，却被某票据中介提前取出，与另外一家银行进行了回购贴现交易，但资金并未回到农行北京分行的账上，而是非法进入了股市，又由于近期A股下跌，导致巨额资金缺口无法兑付。”

在之后不到一周的时间里，2016年1月28日，中信银行兰州分行也爆出9亿～10亿元的票据诈骗事件。

本书在3.1.4小节中已经指出，票据业务领域的乱象非常多，除了一票多卖等票据违规交易问题，还包括克隆票、假票、变造票等违规操作问题。票据识别、担保信息不透明、风险高、票据质量差等问题已经成为票据理财的威胁者。中汇在线、农业银行北京分行以及中信银行，都是这些威胁者的牺牲品。随着区块链智能合约的兴起，更多人将票据理财安全的重担寄希望于它的身上。

在票据理财业务中，银行的承兑汇票是安全的基本保障，而最大的风险来自于票据的真假和交易信息的不对称。而区块链智能合约将会保证参与者有能力查看区块链上的各项操作信息。

金银猫运营总监葛雷称：“一旦区块链技术运用到票据理财中，将彻底杜

绝票据理财交易中的票据作假、一票多卖等现象，同时可追踪票据兑付时间及主体，以保证各方的利益。”

当区块链智能合约被运用到票据理财交易中，票据从申请、发行、交易到承兑，整个过程中的所有环节都将被完整记录下来，并且无法篡改。监管部门可以很方便地查询，如果票据被非法占有，区块链智能合约上将显示出票据的转移路径，有利于将其找回。

然而，要实现以上设想，前提是由数字化契约形成数据票据池。票据的发行方、流通方等必须按照区块链智能合约的规则将票据进行登记和数据备份。

从表面上看，区块链智能合约将会解决票据理财的风险敞口，但事实并非如此。区块链本质上只是一种互联网技术，其作用是将票据信用转化为数字信用，并没有改变票据的金融属性。利用区块链智能合约可以降低票据理财的风险，但依然离不开风控。

盈灿咨询数据组组长杨凌驰表示：“目前区块链技术只是一项新的金融工程，我们可以把它想象成是一个公共账簿，拥有为系统数据提供可靠架构、为互联网金融建立信任关系等特点。这样可以在比较大的程度上改善信用问题，但是其依然不能代替风控，至少目前是无法实现的，未来的路依然漫长。”

票据宝 CEO 李华军的观点更加明确，称：“当前的区块链根本不可能运用到票据理财交易中，因为区块链技术在国内金融体系内还没有任何应用，国内当前仍然以纸质商业汇票为主，电子商业汇票只在人民银行大额支付清算系统中流转，数据对外完全是封闭的。”

我们无法否认李华军的观点，但是探索区块链智能合约在票据理财领域的应用依然显得很有必要。对于区块链智能合约应用在票据理财领域后的未来，我们表示期待。

Block chain

第4章
区块链与数字货币

区块链诞生于比特币，而以比特币为首的数字货币是区块链当前最主要的应用。自从2009年比特币诞生以来，基于区块链技术底层技术的数字货币在全球兴起热潮，并以颠覆世界的姿态冲击着人们对以传统货币为主体的现代金融体系的认知。本章一起了解区块链与数字货币的知识。

practice

4.1 货币的终极形态——数字货币

对很多中国人来说，手机支付已经成为日常生活不可或缺的一部分。即便是二三四线城市，依靠一部手机也可以完成衣食住行，包括吃饭、打车、看电影、订酒店等。在手机支付过程中，人们使用的货币形态是电子货币。货币就像一种活的生物体，在不同的时代环境下进化和演变出不同的生命形态，从贝壳到黄金白银，再到纸币，再到电子货币，最后到数字货币。尽管当下我们对电子货币已经习以为常，但是纵观整个人类货币体系，我们很有可能已经迎来了货币的终极形态——数字货币。

4.1.1 货币自身形态进化论

自人类诞生以来就出现了价值交换，这也是货币自身形态进化的基础。人类历史发生了翻天覆地的变化，除了科技的巨大驱动以外，货币形态的进化也起到了巨大作用。下面一起看货币自身形态进化史。

在原始社会，人们主要以打猎为生，于是产生了最原始的价值交换方式——物物交换。这种交易方式难以满足人们对公平的需求，比如一个人试图用自己饲养的一只羊换另一个人饲养的一头牛。

当人们意识到物物交换烦琐而复杂的时候，作为交易媒介的实物货币开始出现。实物货币诞生的时间是原始社会末期。一般来说，游牧民族以牲畜、兽皮类来实现货币职能，而农业民族以五谷、布帛、农具、陶器、海贝、珠玉等充当最早的实物货币。据考古发掘，新石器晚期遗址陕西西安半坡出土大量陶罐作为殉葬物；大汶口文化遗址殉葬大量猪头和下颌骨。这些殉葬物表明在原始社会后期猪和陶器曾起过货币的职能。

然而，最早充当货币功能的实物流通范围较小，而随后出现的贝壳是流通最为广泛的古代实物货币。因为牛、羊、猪等牲畜充当实物货币不能分割，而五谷的保质期较短，而珠玉又比较稀少，刀铲等农具较为笨重，因此最后的实物货币集中为贝壳。漂亮的贝壳可以用作颈饰，体积小，便于携带与计数，而且还非常坚固耐用，因此在长期商品价值交换中被选为主要货币。作为实物货币，贝壳一直沿用到春秋时期。因此，很多与价值、财富有关的中国汉字都与“贝”字有关，比如财、资、贵、贫、贪、购等。

春秋战国时期的商品经济急速发展，贝壳因为数量有限已经无法满足人们在日常商品价值交换中的使用，于是，金属称量货币开始出现。金属称量货币在流通中需要分割和鉴定成色，使用起来比较麻烦，因此金属铸币逐渐取代了金属称量货币。

政治统一要求经济统一，于是秦统一六国后，秦始皇顺应历史发展趋势，在统一文字、度量衡的同时，也统一了货币。秦始皇规定以“黄金”为上币，以镒（相当于 20 两）为单位，以圆形方孔铜钱为下币，以半两为单位。钱文“半两”的实重为半两，这种圆形方孔的铜钱从此成为中国货币的主要形式，一直沿用两千多年。秦朝的圆形方孔铜钱是世界上最早由政府法定的货币。

金属货币也存在一些问题。动辄好几十斤的金属货币在运输时会耗费很多的时间和精力，于是北宋时出现了纸币。在货币史上，纸币的出现是一个重要转折点，也是人类历史上的一大进步。纸币出现在北宋具有一定的必然性，因为它是社会政治经济高速发展的必然产物。

众所周知，宋代的商品经济空前繁荣，商品的价值交换也异常频繁。频繁的商品交易活动需要用到更多的货币，而当时铜钱短缺，已经远远无法满足流通用量。当时的四川地区通行铁钱，铁钱量重值低，使用起来非常不方便。当时的一个铜钱相当于十个铁钱，一千个铁钱的重量为大钱 25 斤，小钱 13 斤。当时的人如果想要到集市上买一匹布，大概需要铁钱两万，重量为 500 斤，如果没有车根本过不去。

作为宋代的经济重地，成都通往外界的道路异常崎岖难行，客观上需要更为轻便的货币，这就是纸币最早出现在四川的主要原因。另外，尽管北宋是一个高度集权的封建专制国家，但是没有统一的全国货币，而是由几个货币区各自为政，互不通用。当时，4 路专用铁钱（宋代的行政单位），13 路专用铜钱，

陕西、山西则是铜钱、铁钱兼用。而各个货币区都严禁货币外流，纸币的出现正好可以防止铜钱、铁钱外流。

此外，宋朝政府与夏、辽、金的关系紧张，经常受到这三个国家的侵略，于是需要用到大量的军费和赔款开支，这也要求宋朝政府发行纸币来弥补财政赤字。总之，种种原因促成了纸币的产生，而纸币在当时被称作“交子”。一般来说，人们通过钱庄兑换交子。

1688 年，英国发生光荣革命，从此进入君主立宪制。到 1717 年，英国政府建立了事实上的标准化金本位英镑，货币的标准化影响了全球各个国家，也是人类货币史上的重大进步，直接促进了工业革命的发展，使英国成为当时的世界霸主，人称“日不落帝国”。

信息革命爆发后，电子货币出现了。Digicash 公司发明匿名数字货币的技术宣告电子货币诞生。1995 年 10 月，第一家网络银行在美国成立，随后推出各种电子货币。

电子货币的产生和流通使实体货币与观念货币发生分离，解决了经济全球化背景下降低信息成本和交易费用的问题。电子货币突破了空间限制，使信息流、资金流可以通过网络迅速、便捷地传输。总之，电子货币的出现加快了经济全球化，使人们可以更快、更省地处理经济事务。

2008 年，全球经济危机爆发，中本聪在网上发表《比特币：P2P 电子货币系统》论文，描述了比特币的模式，并搭建起比特币体系。之后陆续出现的莱特币、约克币等数字货币的相继出现标志着人类历史进入数字货币时代。

数字货币是货币自身形态进化史的一部分，是数字科技革命的结晶，其诞生具有必然性。回顾人类历史，任何一种新事物从诞生到发展成熟，都会经历质疑乃至排斥。

与传统货币一样，数字货币也将不断发展完善，最终走向成熟，以更适应社会生产力并为人类服务。目前来看，数字货币应当是人类货币的终极形态。

4.1.2 数字货币的零通道费用

2014 年 12 月 14 日，“三亚·财经国际论坛”在海南省三亚市召开。火币

网创始人兼 CEO 李林作为数字货币的一个从业者，向大家介绍了数字货币近几年的发展状况以及大家对于这个行业的未来预期。

李林称："人民币和美元本身在国际上两大货币，中国跟美国也是两大经济体，而在数字货币领域，中国和美国依然是两个领头市场。中国目前的主要产业集中在生产环节和货币兑换环节，美国集中在流通以及存储的环节。再看全球范围内主要的经济体，英国美国日本实际上基本政策差不多。美国考虑更多的是如果将其当作商品怎样进行征税，英国更开放一点，认为这个是私人金钱或者私人货币，但日本目前没有这个法规。"

纵观全球，数字货币与 20 世纪 90 年代初互联网行业的发展情况非常像，任何新技术的发展也都会经历这一历程。从新技术的发展曲线来看，数字货币还处于一个很早期的阶段。

那么，数字货币对现有的金融体系会带来什么挑战呢？与法定货币 7% ～ 8% 的通道费用相比，数字货币的通道费用几乎为零。作为一个去中心的低成本通道，数字货币挑战了当前的跨境支付体系。

关于当前的跨境支付体系，本书在 3.1.1 小节中有具体讲述，这里不再赘述。

4.1.3　顺应经济全球化趋势的全球流通特性

经济全球化趋势的逐渐加强要求一种具有全球流通特性的货币去进行全球贸易，同时，如果由一个国家发行这种全球流通货币，结果就是极大地增加不同国家之间的交易成本。

假设 A 国的货币充当全球货币，那么，B 国和 C 国进行贸易的时候都必须先向 A 国出口他们所能出口的东西，拿到 A 国货币，然后 B 国和 C 国才能用 A 国货币进行贸易。也就是说，凡是 A 国之外的其他国家进行贸易，都必须先对 A 国进行出口换取货币。在这个假设中，只有 A 国全体国民享受了隐形的货币收益。如果 A 国又发生了通货膨胀，那么 B 国和 C 国付出的成本将更多。

一旦 A 国从全球贸易中获取的收益难以支撑货币成本，那么随着货币使用范围的收缩，全球贸易体系将面临崩溃。更致命的打击是，一旦 A 国之外的另一个国家 D 建立了一个足够齐全的工业门类和巨大规模的工业生产，那

么其他国家拿着D国的货币从D国购买商品，那时，A国的货币将成为增加全球贸易成本，阻碍全球商品流通的东西。

数字货币的到来使以上问题都不复存在。数字货币将以一种全新的方式创造人类经济活动的高峰。作为数字货币的代表，比特币创建了人类第一个经济共和。

在比特币系统里，人人拥有平等的经济地位，而且可以随时加入或退出。只要满足基本的通信条件，哪怕只有一个可以上网的余额仅剩1元的智能手机，无论多么巨大的资金量，都可以在10分钟内完成全球任意位置的转移。比特币系统实现的资源配置不仅仅指资金的资源配置，这里的资源远远超越货币的范畴。

举例来说，美国和欧洲曾对伊朗进行经济封锁，导致伊朗的石油无法走出国门，极大地影响了伊朗的经济。然而有了比特币之后，伊朗可以直接利用石油燃烧发电，然后将大量的电用来“挖矿”。通过一个简单的网络通信，伊朗可以将庞大的石油财富转化成比特币，然后在10分钟内到任何一个交易所进行兑现，换成外汇。这样就打破了美国和欧洲的经济封锁。

货币承担的主要功能是价值流通，而数字货币可以完美地承接这一功能。作为安全度高、全球通用、大小额度通吃的价值流通介质，数字货币甚至可以满足人们任何形式的资金调度。数字货币或将成为人类最便捷的全球性资源配置工具。

4.2 比特币能买到的酷炫商品

在第一章开头，我们就讲述了数字货币的龙头老大——比特币。作为全球流通市值最大的数字货币，比特币已经可以用于现实购物。下面一起看比特币可以买到哪些酷炫商品。

4.2.1 午餐用比特币订比萨

现实世界里第一笔比特币交易就是用于购买比萨，美国佛罗里达州程序设计员拉斯洛•豪涅茨(Laszlo Hanyecz)就是交易者。2010年5月21日，拉斯洛•豪

涅茨用 1 万个比特币换了一张比萨连锁店棒约翰的比萨优惠券，这张优惠券价值 25 美元。当时的折算比率大致为 1 比特币 =0.015 元人民币。

如果拉斯洛·豪涅茨的比特币保存至今天，至少可以换得 4 000 万人民币，因为比特币已经升值了数十亿倍。

如果你身处美国、英国或者澳大利亚，你也可以使用比特币购买比萨。PizzaforCoins 是一家专门做用比特币购买比萨交易的创业公司。当前，网站的使用仅限于美国、英国、澳大利亚，加拿大地区正在开发中。你只需要选择你的国家，就可以看到当地与这家公司合作的比萨品牌。比如，选择美国，就会出现达美乐比萨、必胜客和棒约翰三家比萨品牌。用户选择自己喜欢的一家，就可以开始点餐了。

必胜客一个大份鸡翅的价格为 0.06 个比特币左右，按照 2016 年 6 月 1 日一个比特币价值 550 美元的市值计算，也就是 33 美元。然而，你只需要用比特币支付就可以了。

在 PizzaforCoins 网站首页上有详细的“购物指南”，与一般网上订餐的流程相似，用户直接单击“现在就订餐”就能进入下一个页面。预订时，用户需要输入名字和住址，然后网站就会跳转至订单界面，上面有比萨类型、用比特币标注的价格等详细信息。选好这些后，待 Pizzaforcoins 确认支付成功，10 分钟内就可以生成订单了。

PizzaforCoins 的创始人是 Matt Burkinshaw 和 Riley Alexander，他们在网站“关于”部分称，他们创建网站的目的是扩大比特币在现实世界中的使用范围。Matt Burkinshaw 和 Riley Alexander 都非常喜欢比萨这款意大利美食，对于是否要成为一个盈利企业，他们还没有任何表示。

随着 PizzaforCoins 的火爆，很多餐厅都开始支持用比特币付款。比如，在网站 Bitcoin Restaurants 与 PizzaforCoins 类似，支持用比特币进行线上订餐，而且还将业务扩展到了餐厅。网站 Bitcoin Restaurants 的合作餐厅分布在 23 个州，其中加州最多，有 18 家餐厅都与这个网站合作。

4.2.2　比特币支付，戴尔、苹果都支持

2014 年 7 月 18 日，戴尔公司正式宣布用户可以在戴尔网站上使用比特币

进行支付交易。在戴尔网站上，用户可以用比特币购买任何喜欢的戴尔商品。截至 2017 年，这一功能还只限于美国消费者以及一些小企业，在未来将会向国际市场推广。

戴尔公司称，作为一种新型的支付方式，比特币可以为用户提供更高的灵活度。公司 CEO 迈克尔·戴尔（Michael Dell）表示："比特币支付能在世界上任何地方轻松进行，可降低支付处理成本。用户可完全控制比特币，因此其比特币账户无须与任何金融机构挂钩、不会被冻结且交易费用低于多数信用卡。"

据了解，戴尔公司与 Coinbase 联手为戴尔用户提供了比特币付款方式。购买过程与一般网购类似，用户仅需三个步骤就能实现用比特币支付，内容如图 4-1 所示。

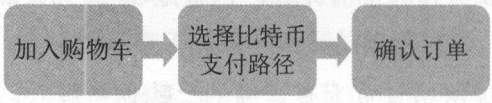


图 4-1　戴尔用户使用比特币支付的三个步骤

第一步：加入购物车。当你登录戴尔网站，准备购买看好的商品时，首先要将购买的商品添加到购物车，然后填写送货单，并选择比特币作为支付方式。当你提交订单时，页面会自动转至 Coinbase.com 完成购买。

第二步：选择比特币支付路径。转至 Coinbase.com 以后，你需要选择比特币的支付路径。这里有两种选择：一是利用自动生成的付款地址或利用智能手机扫描 QR 码，直接通过比特币钱包进行支付；二是登录之前设置好的 Coinbase 账户并直接支付。

第三步：确认订单。支付完成后，你将会返回到戴尔网站上确认订单。在戴尔网站上使用比特币支付的整个过程是非常简单的。

另外，戴尔公司为了庆祝推出比特币支付功能，对所有使用比特币购买戴尔商品的客户提供 10% 的优惠（最高不超过 150 美元）。

戴尔公司全线支持比特币交易成为继苹果公司之后，表态支持比特币交易的又一大科技公司。

就在 2014 年 6 月初，也就是苹果公司召开 WWDC（苹果全球开发者大会）

期间，苹果公司更新了 App Store 商店的审查指南。根据指南的第 11.17 条显示："只要不违反当地的法律，应用程序可以允许虚拟货币进行传输。"这意味着苹果公司可能允许使用比特币在 App Store 商店内购买应用。

审查指南更新后，App Store 上线了首款比特币应用 Coin Pocket。这款应用允许用户收发比特币、查看价格、收集资产并进行加密。这一举动说明苹果公司允许比特币应用进入 App Store。在不远的将来，苹果公司对比特币应用的态度将会更加开放。

4.2.3　用比特币全额购买特斯拉Model3

2016 年 4 月 5 日，比特币已经从最初可以订比萨到全额购买一辆新型汽车了。BitGo（比特币安全平台）的软件工程师梅森·博尔达（Mason Borda）就使用比特币全额购买了一辆特斯拉 Model3。

梅森·博尔达在自己的博客上发文说"我刚刚预订了一辆特斯拉 Model3，并用比特币付了全款"。他还解释了自己如何发现并看中了这款超酷的特斯拉汽车以及他是如何用比特币从电动汽车制造商那里买下了这辆车。

梅森·博尔达预订这辆车时，并没有直接将比特币发送到钱包地址，也没有使用特斯拉网站提供的比特币支付网站，而是利用了传统的法币支付渠道，使用比特币在汽车制造商的网站上支付。梅森·博尔达首先使用 ShakePay（利用比特币购买信用卡的比特币应用）创建了一个信用卡，并向其中存入了价值 1 000 美元的比特币，用于支付预订汽车的款项。支付完预订款后，他又支付了剩余的价值 34 000 美元的比特币，预计 2017 年年末就可以提车，如果特斯拉公司不延期交付的话。

截至 2016 年 10 月，梅森·博尔达购买的这款特斯拉 Model3 汽车预订名额已满，而且公司表示两年内不再启动预订工作。

比特币的商品的交易范围不仅限于比萨、戴尔商品、苹果应用、新型汽车，购买飞机票、住酒店等都可以使用比特币。

拉脱维亚波罗的海航空公司（airBaltic）接受比特币支付，其官网上有比特币通道。目前，该航空公司支持飞往中国、越南、俄罗斯、冰岛等 60 多个

目的地，支付范围仅限于最低价位的机票。airBaltic 是全球第一家支持比特币支付的航空公司，如果你想去三亚过冬，通过官网 airBaltic 就可以直接订票，与他们合作的第三方支付机构 Bitpay 负责比特币的汇率兑换处理。

另外，美国加利福尼亚迪士尼乐园的 Howard Johnson 酒店的老板 Jefferson Kim 是一个比特币爱好者，他的酒店就支持比特币订房。如果你恰好在美国出差，想要住在 Howard Johnson 酒店，就可以用比特币在酒店官网上进行预订。其官网详细地介绍了应该如何用比特币来订房的流程。另外，一家在线的旅游网站 Expedia 是第一家接受比特币的主要旅行机构，用户可以在这里进行酒店预订。

也许在不久的将来，比特币的使用范围将会更加广泛，比特币的价值会更高，让我们拭目以待。

4.3 数字货币新前沿——以太坊

以太坊（Ethereum，ETH）是一个平台和一种编程语言，开发人员可以在平台上建立和发布下一代分布式应用。在比特币这个先行者的基础上，以太坊则正在拓展新的领域，在决策层面和执行层面都是这样。比特币有意限制了其脚本语言，以太坊的编程语言却可以让大家实现更多的功能。另外，以太坊的系列化开发工具也受到了开发者追捧。最重要的是，以太坊在尝试许多全新的事物，虽然大部分都在实验中，我们可以看到来自世界各地的开发者做出的应用程序列表。目前，这个列表正在迅速扩充中。以太坊在一定程度上代表了数字货币发展的最前沿。

4.3.1 以太坊的发行模式

作为一种数字货币，以太坊是推动以太坊平台上分布式应用的加密燃料。

与比特币一样，以太坊通过挖矿的形式发行，但是每年的发行数量保持不变。以太坊每年的发行数量是预售以太坊总量的 0.3 倍。

尽管以太坊每年的发行数量一定，但是货币总量增长的速率并不是固定的。每年都会有一定数量的以太坊因为私钥丢失而损失，损失比率达到 1%。比如，拥有者在去世前没有把私钥告诉他人或者故意将以太坊发送到没有私钥的地址中，造成以太坊数量上的下降。

如果我们假设在预售时会卖出价值 10 万比特币的以太坊，每一比特币的价格等于 600 以太坊，那么将会有 60 000 000 以太坊在创始区块中被创造出来和分配给购买者。因为以太坊每年的发行数量是预售总量的 0.03 倍，因此每年都会有 18 000 000 个以太坊通过挖矿的形式发行。

考虑到新发行的数量和丢失比率，以太坊第一年的通货膨胀率是 22.4%，第二年是 18.1%，第十年，通货膨胀率降到了 7.0%。第三十八年，通货膨胀率是 1.9%，第六十四年降到了 1.0%。以太坊存量以及通货膨胀率随时间变化的趋势如图 4-2 所示。

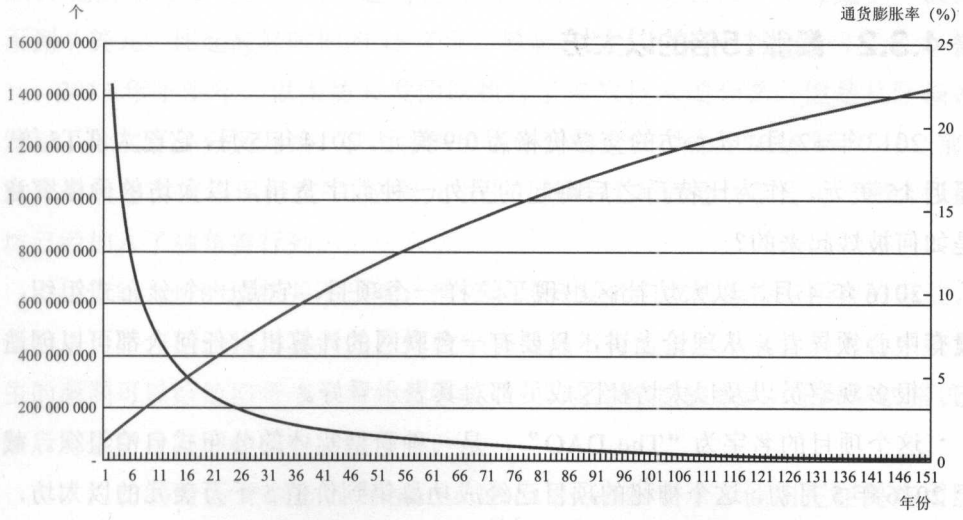


图 4-2　以太坊存量（个）以及通货膨胀率（%）随时间变化的趋势

大约在 2140 年的时候，比特币几乎停止发行。由于每年都会有一些比特币丢失，所以比特币的总量将会不断下降。与此同时，以太坊每年丢失的速度

将会与发行速度达到平衡。

在动态平衡的情况下，以太坊的现存总量将不再增加。如果经济扩张造成以太坊需求持续增长，那么价格将会进入通货紧缩机制。以太坊系统对通货紧缩的抵抗力是非常强的，因为以太坊可以无限细分。只要通货紧缩不是特别剧烈，价格机制会做出调整保证以太坊系统平稳运行。

在法币肆意增发的时代，人们更渴求的应当是一种最终可以充当相对稳定的价值存储器的数字货币。以太坊认同这一价值，并试图在这一核心价值主张下发展壮大起来。

以太坊深刻地认识到，一个基于共识的分布式应用平台必须注重包容性。而保持一个具有搅动作用的发行系统是培育包容性的根本方法。以太坊系统的开发者可以购买或者开发新的以太坊，不论他们生活在2017年还是2027年。

我们相信，恒定的以太坊发行将使利用以太坊在以太坊经济体系内创建企业比投机性存币获得的利益更大，尤其是在以太坊发展的早期。

4.3.2 暴涨15倍的以太坊

2013年12月，以太坊的交易价格为0.9美元。2014年5月，它已大涨15倍，逼近15美元。作为比特币之后崛起的另外一种数字货币，以太坊的价格究竟是如何被炒起来的？

2016年4月，以太坊社区出现了这样一个项目，它是一个分布式组织，没有中心领导者。从理论上讲，只要有一台联网的计算机，任何人都可以创造它。很多观察员以及以太坊社区成员都对其表示看好。

这个项目的名字为“The DAO”，是一种新型实体的分布式自治组织。截至2016年5月初，这个神秘的项目已经成功募集到价值5千万美元的以太坊，在世界众筹金额排行榜上名列第二，仅次于游戏项目star citizen（星际公民）。目前，The DAO是支持以太坊相关项目的主要工具之一。

The DAO相当于一个以太坊流通枢纽，通过发售代币以及投票权募集以太坊，然后将募集到的以太坊依据规则分给其他创业公司以及项目。在The

DAO 项目发布时，Slock.it 区块链公司以及 Mobotiq 共享式电动汽车网络构建公司已经被列为项目潜在的承包商。

与拥有指定管理结构的传统公司不一样，The DAO 的运作模式是集体投票。用以太坊购买 The DAO 代币的人就是项目股东，他们收到的分红有可能包括以太坊。以此为基础，The DAO 代币的持有者通过选举决定项目的监护人有哪些，而且监护人随时可能发生变化。目前，以太坊创始人 Vitalik Buterin 就在 The DAO 的监护人名单中。

然而，关于 The DAO 项目的确切起源，至今无人知晓。那些参与这一项目代码的贡献者们构成了一个错综复杂的关系网络。Slock.it 公司的联合创始人兼 CEO Christoph Jentzsch 是 The DAO 项目开源框架的创造者。

据 Christoph Jentzsch 说："没有人知道是谁发起了这个项目，包括我。当然，我们可以在区块链上看到这个地址，但是我们无法知道这个地址的拥有者是谁。与 The DAO 对话的唯一方式，就是提出意见，并进行表决。"

The DAO 项目将以太坊的价格推至顶峰。2016 年 12 月，以太坊分叉 ETH 链面临垃圾交易攻击问题闹得沸沸扬扬，以太坊的价格持续走低，最低不到 7 美元。比起高峰时期的 15 美元，跌幅超过 50%。

2016 年下半年，以太坊开发团队执行了多次技术硬分叉，但是从区块链发生了一次意外分叉开始，以太坊的价格便开始走低。截至 2016 年 10 月之前，以太坊的总市值还保持在 10 亿美元以上。假设以太坊是一家公司，那么以太坊已经加入了独角兽行列。

尽管以太坊的现状并不乐观，但以太坊开发者们依然保持着乐观的看法。他们认为，包括比特币在内的任何数字货币都不可能长盛不衰，以太坊系统发生的漏洞可以给他们带来宝贵的经验教训。只有总结经验教训，采取解决措施，然后有效防止类似的事件再次发生。

以太坊基金会安全负责人 Martin Holst Swende 表示，他们正在提高团队的检测、分析、沟通以及合作能力。除此之外，以太坊开发团队正在研究一种"事后剖析"报告，概述各种以太坊漏洞中得到的经验教训。

在 2017 年，以太坊分叉 ETH 链将会进行共识算法的重大更改，新的共识算法 Casper 相当于模仿工作量证明机制的权益证明变种算法。可以预见，以

太坊分叉 ETH 链将会再次受到重大考验。

以太坊创始人 Vitalik Buterin 提醒大家："以太坊所处的领域是一个新兴且不断发展的高度技术领域。在您选择参与之前，您应该认识一下风险有多高，包括无法预测的系统漏洞风险以及其他技术带来的风险……如果您选择使用以太坊平台，那么您将会承担这个新兴平台的风险，这是必然的。"

4.3.3 比特币VS以太坊

通过上面两个小节的介绍，我们知道以太坊与比特币的发行规则不同，那么两者的交易和投资方式有什么不同呢？

自从以太坊诞生以来，就被视为比特币的有力竞争对手。然而，技术专家和连续创业的企业家 AndreasM. Antonopoulos（著有《精通比特币》一书）认为，以太坊不会是比特币的竞争对手。这一观点引发了业界对比特币与以太坊的激烈讨论。更多人开始关注比特币与以太坊的不同，并讨论两种数字货币在交易和投资方式上的不同。

ARK 投资管理公司的分析员和区块链产品主管 Chris Burniske 认为："比特币主要是在投资方面用于保值，而依靠以太坊网络执行智能合约的以太坊则更多地被视为一种交易工具。"

比特币和以太坊系统都是基于区块链技术建立的。两者的共同特征是交易公开记录，货币及资产交易便捷优惠，没有第三方中介的参与。

截至 2016 年 5 月，全球范围内的比特币 ATM 机数量为 670 台，支持比特币支付的销售点有成千上万个。在这方面，以太坊由于发展较晚，所以在电子支付领域还没有崭露头角。当前，以太坊的主要用途是支撑以太坊网络运行程序。

Strength in Numbers Foundation 的执行董事 David Duccini 说："用户对以太坊的期望与比特币有所不同。两种加密货币都可以进行投机买卖，但是以太坊的原始功能是支撑应用程序运行。因此用户需要足够多的以太坊运行自己的 APP。"

以太坊是作为比特币的竞争对手超越比特币，还是在其他领域走出自己的

发展路径，只能留给时间去验证。

4.4 比特币赚钱效应延伸——莱特币

与比特币类似，莱特币（Litecoin）也是一种基于区块链技术的数字货币。根据 2017 年 2 月 10 日实时行情，莱特币的价格在 26 元附近波动。作为公认的与比特币最相近的数字货币，莱特币延伸了比特币的疯狂赚钱效应，诱发了市场的投资热情。

4.4.1 莱特币的发行模式

莱特币的创始人是前谷歌程序员李启威，预期产值为 8 400 万个。与比特币不同，莱特币网络每 2.5 分钟就可以处理一个区块，交易确认的速度更快。

莱特币的发行模式与比特币相似，由一个 P2P 网络通过 Scrypt 工作量证明机制来处理莱特币交易、结余以及发行。挖矿过程即通过计算机显卡进行哈希运算，如果出现“爆矿”值，系统会一次性奖励 50 个莱特币。莱特币的发行速率按照等比数列每四年减少一半，最终达到总量 8 400 万个。

由于当前的计算机算力增长迅速，矿工利用几台计算机已经很难挖到莱特币，因此需要加入矿池。矿池集合的算力巨大，计算出“爆矿”值的概率也更高。

下面总结了莱特币区块链的三个特点，内容如图 4-3 所示。

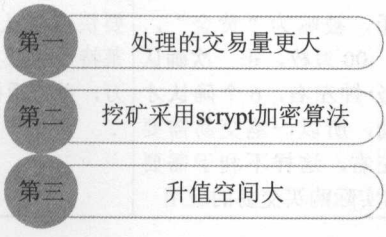


图 4-3　莱特币区块链的三个特点

第一个特点是处理的交易量更大。莱特币网络每 2.5 分钟就会生成新的区块，而比特币需要 10 分钟，因此莱特币区块链中区块的生成更加频繁。如果区块大小相同，莱特币网络就可以支持更多的交易，而且不需要修改软件。

第二个特点是挖矿采用 scrypt 加密算法。莱特币采用的共识机制为工作量证明机制，加密算法为 scrypt 加密算法，所以莱特币适合显卡挖矿。

第三个特点是升值空间大。目前，莱特币的价格为每个 26 元左右，比起比特币 6 600 多元的价格，莱特币还存在较大的升值空间。

不过，从当前来看，还没有较大型的矿场进行莱特币挖矿，但随着区块链技术的发展，数字货币将会受到社会关注并真正投入到实际应用中。届时，莱特币将延伸比特币的赚钱效应。

4.4.2 比特币VS莱特币

除比特币以外，莱特币是最正规和受到最多支持的数字货币。国内外多个平台支持莱特币交易，还有一些国家支持莱特币在 ATM 机上取款。

为了帮助大家对投资比特币和莱特币的价值做出判断，我们将比特币与莱特币进行了对比。比特币与莱特币的主要区别如表 4-1 所示。

表 4-1 比特币与莱特币的主要区别

项目	比特币		莱特币
相同点	都是一种由开源 P2P 软件产生的数字货币，主要特点有：去中心化、全世界流通、专属所有权、低交易费用、无隐藏成本、跨平台挖掘，由于完全去中心化，没有发行机构，也就不可能操纵发行数量		
不同点	算法	比特币是最早出现的虚拟币，也是最多人认同的有金融投资价值的数字货币，被喻为“黄金”，总量只有 2 100 万枚。每一次确认时间为 10 分钟左右，6 个确认才算交易成功，所以一笔交易需要一个小时左右，这样不利于需要快速确认的实际购买交易的应用	莱特币在比特币的算法基础上进行优化，确认时间只要 2.5 分钟，有利于需要快速确认的实际购买交易的应用。莱特币总量是比特币的四倍，即 8 400 万，莱特币被喻为“白银”

续表

项目	比特币		莱特币
不同点	价值	升值空间小	如果按照总价值相等计算，莱特币的价格应当为比特币的 1/4。举例来说，比特币价格是 6 000 元，莱特币就应当为 1 500 元。从目前价格来看，莱特币的价格上涨空间非常大
	实际商业应用	非常广泛	市场价值总量没有比特币多，容易受平台和庄家控制，价格波动可能会比较大，实际商业应用没有比特币广泛

莱特币矿工认为，莱特币的价值上升将会使比特币更具有价值。参考比特币的发展历史，我们可以确信莱特币的价值将继续增长。

Block chain

第5章
区块链在金融领域的应用

世界经济论坛预测，到2027年，世界各国的国内生产总值（GDP）将有10%以上被存储在区块链上。这种预测并不夸张，因为作为数字货币比特币的底层技术，区块链首先将会对现有的金融领域产生颠覆性影响。下面具体分析区块链在金融领域有哪些应用。

practice

5.1 价值资产符号化

区块链技术可以将实体世界的资产和权益进行数字化，并实现 P2P 登记发行、转让交易、清算交割等金融业务。价值资产符号化是区块链对金融领域产生颠覆性影响的第一个表现。

5.1.1 将实体世界的资产和权益迁移到网络世界

想象一下这样的未来：当你起床的时候，用眼睛扫描区块链上的一串符号就收到了来自大连一处海边别墅交易成功的电子确认函。几天后，你来到别墅前，用眼睛扫过大门密码，门就自动打开了。

这套别墅被原来的主人作为数字资产登记在区块链上，当你搜索到这套别墅信息的时候，区块链联合智能全息投影技术为你提供了可视化的立体呈现。你戴上 VR 头盔，如同置身于别墅，柔软的沙发、温和的海风让你非常享受。于是，你决定将这套别墅买下来。你使用比特币轻松完成了交易，交易数据被储存在区块上。

这就是未来的智能生活。在未来，实体世界里的资产和权益迁移到了网络世界里，作为数字资产存在。区块链的快速发展让我们有理由相信，这种智能生活就在未来的 10 ～ 20 年里。

基于区块链技术的小蚁开源系统让我们看到了区块链在实体资产权益数字化方面的初步应用。

比特币是通过工作量证明机制实现财产权利自治和去中心化的，而小蚁则是通过制定确定规则以可追究责任的方式进行没有自由裁量度的简单事务，所

以不需要追求完全去中心化。对开源程序来说，并不一定每个人都有能力独立编译源代码，所以，只要有少数人进行编译验证，然后将编译好的程序提供给大家下载就行。

在小蚁系统里，记账是一种确定性的简单事务，记账人的权力比比特币矿工的权力小得多。这种设计使小蚁系统将清算确认时间减少到了 15 秒。

在比特币区块链上，发起金融交易到确认挂单成功的时间需要 10 分钟。而小蚁使用的是清算型区块链，即牺牲一部分不关键的信息记录，但是可以获得更好的灵活性、吞吐量以及用户体验。小蚁将区块链仅用作登记发生资产变更的交易，并由此派生出一种新型的去中心化交易模式——“超导交易”。

在“超导交易”模式下，小蚁用户不需要给交易所充值就可以在交易所挂单。在挂单成交后，交易所会把成交的交易信息传播到小蚁协议网络中，并被区块链记录。

例如，用户 A 想要通过小蚁卖出自己持有的某公司股权，他不需要提前将自己的股权转进交易所，只需要在本地通过私钥对委托单进行签名，就可以成功挂单。与用户 B 成交后，用户 B 支付的款项将直接进入用户 A 的钱包，而用户 A 的股权则会直接转让给用户 B，不需要通过交易所中转。

超导交易是一种新形态的交易，由交易所负责撮合信息，区块链负责财物交割。由于超导交易所不涉及用户钱财管理，而且交易指令都有密码学证据，所以超导交易所根本没有特殊权力，不涉及监管当局的前置审批。

另外，用户本身不需要为挂单、撤单指令支付小蚁币。如果挂单成交，交易所会承担支付数据写入区块链所需的小蚁币手续费。随着区块链技术的主流化，超导交易模式很可能会成为包括 A 股在内的主流金融市场的发展方向。

小蚁客户端为用户提供了查询、支付两个密码，用户体验与传统网银一致，用户付出较低的学习成本就能获得良好的安全性。除非用户主动向他人提供数字证书，否则任何第三方都不能获知你的身份。

整个现存的互联网金融生态都是小蚁的目标用户，引入大量实体世界的金融资产是小蚁的现阶段目标。因此小蚁的设计充分考虑了合规要求，定位为一个对接实体世界的区块链金融系统。作为一个去中心化的网络协议，小蚁可以被用于 P2P 网贷、股权众筹、数字资产管理、智能合约等领域。

小蚁实现了用户资产数字化，使任意实体资产的财产权益都能够被编程。相信基于区块链技术的小蚁对传统金融系统具有压倒性的优势，而且还将创造出全新的数字化金融生态。

区块链技术的诞生让现实世界里的事物连接以秒计算，并且可以有效抵抗黑客攻击，各类资产可以直接在互联网上登记、交易且数据永远不可篡改。这种巨大的魅力让各类资产汇聚在区块链上，用公钥和私钥进行资产管理。到时候，我们所有的各种资产都将以符号的形式存在于算法里，人与人之间的信任也存在于算法里。

5.1.2 区块链上的P2P交易所

由于P2P网贷平台风险频发，跑路的P2P企业数量大幅增加，北京、上海、深圳等地均在2016年年初暂停了P2P企业的注册。这一事件充分说明了目前我国的互联网金融、P2P票据企业仍然处于不成熟的状态。

区块链技术应用于P2P票据交易所有四个好处：一是提升票据、资金、理财计划等相关信息的透明度；二是重建公众、政府及监管部门对P2P票据交易所的信心；三是降低P2P票据交易所的监管成本；四是推进服务实体的经济发展。

下面是依托区块链技术设计并研发P2P票据交易所的方案概述，内容如图5-1所示。

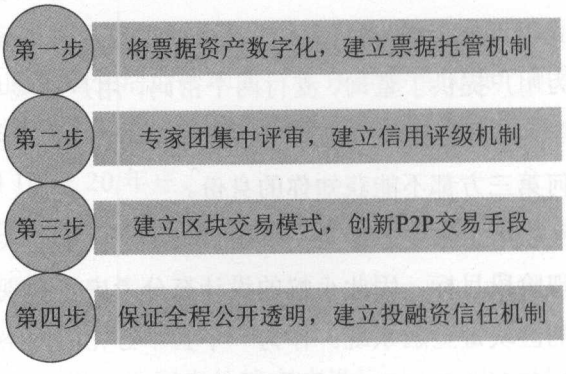


图5-1 依托区块链技术设计并研发P2P票据交易所的方案

第一步：将票据资产数字化，建立票据托管机制。

通过区块链技术实现票据资产数字化，然后引入托管银行。在 P2P 票据交易中，由托管银行发布票据托管、托收、款项收回等信息，确保交易资产真实、有效，确保票据的托收及收回款项的及时、准确、可信赖。

第二步：专家团集中评审，建立信用评级机制。

P2P 票据交易所应当积极发挥自身的引领作用，然后找第三方外部专家团集中评审票据承兑人或持票人的信用状况，建立完整的信用评级机制。信用评级机制为 P2P 票据交易所健康、有序发展提供了前提条件。

第三步：建立区块交易模式，创新 P2P 交易手段。

区块链技术可以将 P2P 票据的评级、托管、登记、认购、转让、结清等环节作为一个完整的交易闭环来处理。区块链分布式账本的记账方式可以及时有效地推进 P2P 票据交易的达成，不仅提升了交易效率，还能保证票据及资金的安全。

第四步：保证全程公开透明，建立投融资信任机制。

区块链交易模式保证了全程公开透明，实现对交易所的标的票据、交易资金、托收资金、理财计划实时监控与信息发布，建立了有效的投融资信任机制，为 P2P 票据交易所发展壮大提供了有利条件。

基于区块链技术的 P2P 票据交易所架构分为三层：第一层是区块链底层技术层，记录 P2P 票据交易总账；第二层为协议层，主要包括运行 P2P 票据交易、评级、托管的软件；第三层为应用层，主要为数字化的票据及资金。

基于区块链技术的 P2P 票据交易所的业务流程如表 5-1 所示。

表 5-1　基于区块链技术的 P2P 票据交易所的业务流程

环　节	内　容
提交申请	票据企业向 P2P 票据交易所提交未到期且待转让的票据，双方线下签约
提交信息	票据企业向 P2P 票据交易所提出评级及登记托管需求，并提交票据详细信息、票据托管、理财计划以及交易要求的其他信息
启动票据评级	P2P 票据交易所通过区块链技术同时启动评级及登记托管流程。商业银行根据各自角色在交易平台中分别对待转让票据进行评级或托管
票据托管	对于纸质票据，托管银行需要审验票据真实性并完成托管手续，然后在 P2P 票据交易平台向所有用户发布票据托管信息；对于电子票据，托管银行在完成托管手续后，在 P2P 票据交易平台向所有角色用户发布票据托管信息。

续表

环　节	内　容
票据评级	如果是银行承兑汇票，P2P 票据交易所首先需要在 P2P 票据交易平台上发布票据承兑行信息，系统会自动对比各商业银行的承兑行“黑名单”，然后统计该承兑行纳入黑名单的数据，根据交易所规则自动生成评级，P2P 票据交易平台中所有角色用户便看到了最终的评级结果。如果是商业承兑汇票，P2P 票据交易所需要让持票者根据交易所评级模板提供持票者的基础信息、财务数据、生产经营状况；或者 P2P 票据交易所根据票据企业融资情况要求贷款银行提供相关授信资料、贷后资料。P2P 票据交易所将根据票据企业所在区域，选择本区域信贷专家组成评审团，在 P2P 票据交易平台中采用匿名评审的方式进行信用评级，每位专家的评审结果在评审团内部发布，系统根据交易所评级规则自动计算持票人的信用评级，评级结果在 P2P 票据交易平台中向所有角色用户发布
登记理财计划	票据托管、评级完成后，票据交易所通过系统自动生成理财计划中的唯一编号，并将托管信息、评级信息、理财计划信息写入票据区块中，向 P2P 票据交易平台中的所有角色用户发布
理财认购	票据企业向所有投资角色的客户发布包括票据评级信息在内的理财计划，投资方在充分认识到投资风险后，与票据企业签订智能合约（P2P 票据交易所通过预先设定代码的方式统一制订）然后将资金划入票据企业，并同步向所有角色客户发布转账及认购信息
理财资金划转	票据理财计划发售完成后由票据企业将资金划入持票人账户，并同步向所有角色用户发布发售完成及资金划转信息
份额转让	投资方可以在票据理财计划到期前转让所持有的份额，由待转让方在 P2P 票据交易平台发出转让申请，新投资方确认后，完成资金的划转。转让申请、投资确认、资金划转等流程需向所有用户发布信息
票据托收	票据到期由托管银行发出托收，托收信息由托管银行在 P2P 票据交易平台中发出并通知所有用户
资金划转	票据托收资金收回后，由托管银行将资金划入票据企业，票据企业根据投资份额将资金划入投资方账户，所有资金划转的过程均通知所有的用户

将区块链技术用于票据交易所有利于解决票据 P2P 领域当前的问题，为票据业务创新提供全新的交易平台，为我国互联网金融可持续、健康发展做出有益尝试。

5.2

金融业为区块链布局主力

当金融业遭遇区块链，会碰撞出怎样的火花？各种猜想都可能难以准确描

述这种技术将给金融业以及其他行业所带来的巨大变化。下面看金融业是如何布局区块链，成为区块链主力军的。

5.2.1　支付方式历史演进

五千年前，人们使用贝壳去交换商品；五千年后，人们用一部智能手机来埋单。2017 年，手机支付已经成为不可或缺的支付方式之一。现金、银行卡都可以不在身上，但是手机却是我们出门之前必须带上的物品。支付时代是如何转换的呢？下面一起看从支付方式的演变，内容如表 5-2 所示。

表 5-2　支付方式的演变

时代	代表	发 展 状 况
货币支付时代	现金	人们出门、购物、旅游都不忘随身携带现金。日常储蓄出现存折。人们乐于在现金交易中靠消费找零互验真伪，也乐意靠一手交钱一手交货寻求踏实放心。各阶层的人都有一套辨认假币的方法，包括抖钱、听听声、用手来回捻搓百元大钞正面右侧防伪痕迹，将百元大抖钞放在日光下寻找防伪记号等
信用支付时代	银行卡	1990 年中国建设银行发行龙卡；1991 年中国农业银行发行金穗卡；1992 年深圳发展银发行“发展卡”；1993 年交通银行发行太平洋卡。截至 1994 年年初，全国发卡量达到 400 万、交易额达到 2 000 亿元。与此同时，各商业银行电子化建设同时起步，投资建设了大量的计算机业务处理系统，后来发展到刷银行卡，结账时只需要拿出银行卡片，等待输入密码和签名就可以了
电子商务支付时代	网上银行	当互联网进入我们的生活后，电子商务逐渐代替了上街购物，现实当中的交易发展到网上交易，传统的银行支付变成了在线支付。网购成为消费者的主流购物渠道，网上银行变成了新支付方式。吃、穿、住、行等所有关于人们日常行为习惯的东西都可以网购，同时可以在线支付
手机移动支付时代	支付宝、微信	移动支付成为主流，人们出门不再考虑带不带现金，带不带银行卡，只要有手机有网络，就能轻松消费。在线缴水费、缴电费、手机充值、号码转账、游戏充值、订车票、购买彩票、违章罚款……移动支付遍布于各个行业。微信支付、支付宝等移动支付方式进入大街小巷，悄无声息改变消费者的支付习惯，让消费者动动手指头就可以消费，方便快捷

奥美与知名调研机构益普索（Ipsos）曾联合发布的“无现金生活”报告指出：“在全世界，无现金交易已经成为明显趋势：2014 年，由以色列总理内塔尼

亚胡牵头的委员会探讨制订了一项三阶段计划，旨在消除以色列的现金交易；2015 年，人口少、数字化程度高、手机普及度高的丹麦成为世界上第一个不使用现金的国家；2016 年，瑞典约 80% 的交易以电子支付方式完成，美国约 80% 的消费都通过银行卡成交。在肯尼亚内罗毕和非洲其他地区，无现金交易也正在迅速流行开来，小额贷款组织从 2008 年就开始用一种叫 M-PESA 的移动支付服务放贷。”

2016 年 8 月 8 日，微信支付启动“无现金日”活动。这在一定程度上表明无现金移动支付在中国已经形成一股潮流，无现金日将会成为继“双十一”之后又一标志性的节日。

据了解，微信首个“无现金日”启动于 2015 年 8 月 8 日，各个领域将近 8 万家商户参与其中。随后，支付宝也宣布每年 8 月为“无现金月”，活动方式以商家折扣和补贴的形式出现。2016 年，微信支付“无现金日”的参与商户数量达到 70 万户，是 2015 年的 8 倍多。

可以说，无现金支付是支付方式发展和演变的必然路径。支付及货币体系实质上就是一个庞大的会计记账系统，与互联网及区块链等新技术的结合是必然的。

在后现金时代，支付方式的演进将包括四个方面，内容如图 5-2 所示。

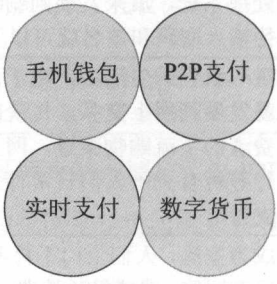


图 5-2　支付方式的演进

手机钱包的发展得益于智能手机的普及，是移动支付的手段。手机钱包需要绑定银行卡，然后才能进行支付。对消费者来说，手机钱包的安全性是一个重要考虑。

P2P 支付指的是个人与个人之间通过手机进行价值转移。肯尼亚的移动货

币支付平台 M-Pesa 就可以通过加密短信来达到汇款及支付的目的。

实时支付技术建立在已有的实时支付基础设施之上，不依赖银行卡。

在数字货币中，比特币是最著名的。作为 P2P 的支付方式，比特币通过区块链的技术得以实现。

当一种支付手段普及后，其便捷性的增强会与普及程度形成正循环，这就是网络效应。从这一角度来看，支付宝与微信支付的覆盖范围已经形成网络效应，开始真正地改变人们的生活方式。当区块链技术的应用真正落地，数字货币支付将产生更大的网络效应。

5.2.2　支付汇款方式变革

纵观超市、饭店以及所有需要交易的地方，支付宝以及微信支付已经成为一种非常常见的付款转账方式。不仅是在一线城市，在二、三线以及四线城市，支付宝以及微信支付都是非常火爆的。

支付宝以及微信支付的火爆程度甚至超过了美国的 Paypal 以及 Apple Pay。在美国，由于信用卡体系非常强大，人们日常生活已经习惯了刷卡消费，所以移动支付在美国的发展非常困难。就连包括日本、中国在内的众多国家都比美国移动支付的渗透率高。

当区块链进入金融业，支付汇款方式将发生重大变革，美国的信用卡体系将会受到更大的考验。下面我们看看区块链技术与移动支付结合到一起后对金融业带来的巨大变化。

首先是移动支付。移动钱包的出现在很大程度上动摇了现金和支票的地位，苹果支付、安卓支付以及零售商提供的数字钱包等移动钱包为用户带来的便利和轻松吸引了众多用户的注意力。然而，移动钱包的安全性一直为人所诟病。区块链技术的多重签名验证购物信息功能为移动钱包的安全性提供了有利保障，同时还可以阻止诈骗行为，如重复支付、欺诈、哄抬物价等。另外，区块链技术还能够提高支付速度、改善用户体验、降低全球支付成本费用。

其次是汇款。据业内人士统计，全球的平均汇款成本在 7% 以上，而商业银行更是远远超过这一水平。如果全球的汇款成本降低 1%，那么全球的消费

者每年节省的费用达到 80 亿美元。由于区块链消除了第三方机构的作用，区块链使这一想法有了实现的可能。区块链与移动支付结合在一起后，将会降低移动用户向世界上任何人进行转账的时候所支付的高额服务和交易费用。比如，Abra 和 Coins.ph 公司就已经使用区块链技术实现了比特币的全球转账交易。

另外，区块链的应用将会弱化银行的作用。据统计，在美国以及尼日利亚，有数百万的华人都没有当地的银行账户。然而，区块链为这些人解决了这一难题。现在只需要一部智能手机，不需要银行账户，他们就可以通过区块链参与全球电子商务、获取贷款或者向朋友、家人等进行安全转账而无须支付高昂的费用。

奖励和忠诚度计划也会因为区块链发生变革。在购物的时候获得奖励是任何一个消费者都喜闻乐见的事情。而移动端就是提供和管理奖励活动的最好平台，星巴克已经证明了这一点。区块链技术可以改善积分交易的方式，因为所有的交易都记录在一个公开的账本上，所有商家都可以监视积分交易。例如，你只需要轻轻一点，就可以把你在航空公司里的积分送给你的朋友。

伦敦初创公司 Plutus 正在研发一款转账或购物时可以获得数字令牌奖励的移动程序。这些奖励回扣可以用在任何接受比特币交易的地方。当这种移动程序普及开来，商家就会使用这种奖励系统来奖励消费者。到时候，你完全可以在航空公司使用在星巴克获得的奖励积分。

随着物联网的发展，支付将变得前所未有的简单。例如，在将来，你走进一家商店去购买矿泉水，只需要晃动一下手，你的智能手表就可以检测到矿泉水瓶上的半透明密码，然后执行一个哈希函数，矿泉水就会立即变成你的。这一切都离不开区块链。

区块链解决了现有金融支付系统的三大问题，内容如图 5-3 所示。

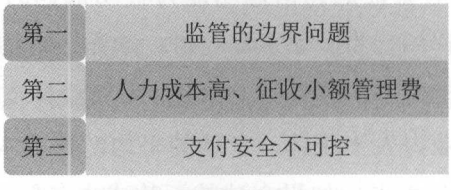


图 5-3　区块链解决的现有支付系统的三大问题

第一，区块链解决了金融业监管的边界问题。《关于促进互联网金融健康发展的指导意见》认为，互联网金融新模式需要众多不同部门的监管。然而，每一个新兴领域都会因为行政资源不足而导致监管不完善以及滞后性。传统行业发展时间长，监管相对完善，已经形成了既有的规则。但是问题来了，当前的规则无法适应互联网下民众的需要。

互联网产业发展非常快而且没有边界，而在传统行业里做同样事情的时候，就会很难实现。简单来说，传统模式是将市场上的产业人为划分为可控和不可控两种。将可控领域的监管方法（比如颁发牌照、例行检查等）用在不可控的领域里起到的作用很小。最大的难点就是不可控领域的边界难以确定。对支付 / 账户 / 资金这些领域来说，用资金的走向来描述边界在理论上非常容易，但在实践上非常难。

从理论上说，任何涉及资金交易的领域都属于监管范围；但从实践上来说，根本不存在一个强大的中心可以掌控所有资金的走向。而区块链解决了电子化交易和实际交易脱节存在的问题。

以比特币为例，比特币交易属于电子化交易，而且可以通过区块链分布式账本进行认证，这就使比特币交易必须是真实的，也不能是脱节的。总体来说，区块链解决了记假账、记账却没有交易、交易却没有记账的问题。

第二，区块链解决了现有金融支付系统人力成本过高、需要征收小额管理费的问题。中国银行业正面临发展“瓶颈”，在这种情况下必须给自己找到突破口。从用户方面来说，银行业受到了第三方支付的冲击；从信贷业务来看，受到了 P2P 网贷平台的冲击；从获得数据的能力来看，银行受到了供应链金融的冲击。

这种现状的造成原因在于改革进程的需要。当市场上的利益分配不合理时，新兴的势力便站出来挑战传统的既得利益者。对银行业来说，应该让自由的市场竞争来引导市场，让创新企业得到发展空间。区块链用技术保障了金融交易的进行，降低了人力成本。另外，记账参与者的目标是从网络中挖掘数字货币，不向交易双方收取管理费。

第三，区块链解决了支付安全不可控问题。区块链建立了一种基于平等的规则，所有的参与者基于同样的规则进行交易，违反规则的参与者不能

完成任何一步任务。在区块链的逻辑中，个体与个体之间的能力更加开放和透明。

在新的金融业态下，银行业务将真正回归存款、借贷的本质。随着区块链技术的应用越来越广泛，自金融时代将真正到来，个人从事金融交易活动可能不再需要任何机构。

5.2.3 票据清算重构

关于区块链重构金融业票据清算系统的原理，我们在 2.3.2 小节、3.4.3 小节中均有所提及，这里不再赘述。下面看区块链对票据清算带来影响的四个方面，内容如图 5-4 所示。

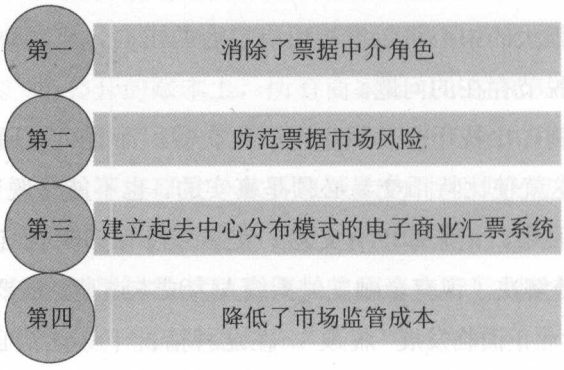


图 5-4 区块链对票据清算带来的影响

第一，消除了票据中介角色。在应用了区块链技术之后，票据价值可以实现 P2P 无形传递，既不需要特定实物作为连接双方取得信任的证明，也不需要第三方对交易双方价值传递的信息做监督和验证。另外，票据交易双方常常需要通过票据中介来解决信息不对称问题，而借助区块链实现 P2P 交易后，票据中介的现有职能将被消除。

第二，防范票据市场风险。不透明、不规范以及高杠杆错配等潜规则使票据市场的风险频发，参与机构的多样性和逐利性也加大了这一风险。而区块链技术的应用可以避免相关风险。

首先，全网公开、数据不可篡改的区块链使得纸质、电子票据一旦交易就不能抵赖，可使用有效方法防范道德风险；其次，区块链分布式系统无须第三方中介，完全避免了人为操作产生的风险；最后，区块链可以自动控制参与者资产和负债两端平衡，并且公开透明的数据使整个市场交易价格对资金需求的反应更真实，进而形成更真实的价格指数，有利于控制市场风险。

第三，建立起去中心分布模式的电子商业汇票系统。现有的电子商业汇票系统（ECDS）是一个中心化系统，其中心为央行，其他银行和企业通过直连或网银代理的方式接入央行的中心化登记和数据交换系统。而区块链技术将会改变现有电子商业汇票系统的存储和传输结构，建立起去中心分布式模式，还能利用时间戳完整反映票据从产生到毁灭的过程，使每一张票据都可以追溯历史。区块链建立起的全新连续“背书”机制将更加真实地反映票据权利的转移过程。

第四，降低了市场监管成本。多样的操作方式使票据市场的监管变得非常繁杂。监管方式只能是现场审核，而业务模式和流转则没有全流程的快速审查和调阅手段。

区块链应用将使票据流转的方向具有可控性，比如，通过程序限定贴现中必须有真实贸易背景、设定资管票据不能绕开信贷规模等。区块链在票据市场中国的应用有利于形成统一的市场规则，建立良好的市场秩序，进一步发挥票据在实体经济中的作用。

5.3 受影响的金融机构及案例

区块链对金融业的影响日渐加剧，金融业将迎来颠覆性变革。在这一过程中，各大金融机构将会首当其冲。区块链将会影响的金融机构包括证券交易所、会计审计机构、金融主管机构、大型科技企业、银行体系等。下面分别看各大金融机构受到的影响以及案例。

5.3.1 证券交易所

在证券交易所中，证券交易的过程包括开户、委托、撮合成交、清算交割、过户等环节。

第一个环节是开户。开户指的是用户要在券商处为自己分别开设一个存放股票及资金的账户，以为股票的交易提供方便。开户之后，才有资格委托券商代为买卖股票。开户时要同时开设股票账户和资金账户。当甲投资者买入股票，乙投资者卖出股票，成交后股票从乙投资者的证券股票账户转入甲投资者的账户，相应的资金在扣除费用后从甲投资者的资金账户转入乙投资者的资金账户。

第二个环节是委托。办理完股票账户及资金账户后，用户便可进入正式的股票交易。由于法律规定一般的投资者不能自己直接进行股票买卖，股民所有的股票交易都必须通过券商进行，这就是委托。

第三个环节是撮合成交。券商在接受了投资者委托后，就可以通过专线电话与派驻在交易大厅内的代表人联系，或者直接通过先进的计算机和通信系统将用户的委托内容报告与证券交易所内的自动撮合系统参加集合竞价或连续竞价。证交所内的交易系统根据时间优先及价格优先的原则，对符合条件的委托予以成交，这个过程就是撮合成交。股票成交后，证券交易所随后将成交记录反馈给券商，券商再通知股民在指定的交易日进行确认。

第四个环节是清算与交割。清算与交割是一笔股票交易达成后的后续处理，是价款结算和股票交收的过程。清算和交割是股票交易中的关键一环，它关系到买卖达成后交易双方责权利的了结，直接影响到交易的顺利进行，是市场交易持续进行的基础和保证。

第五个环节是过户。我国证券交易所的股票已实行所谓的“无纸化交易”，对于交易过户来说，结算的完成即实现了过户，所有的过户手续都由交易所的计算机自动过户系统一次完成，无须投资者另外办理过户手续。

在传统股票交易过程中，用户需要支付印花税、佣金、过户费、委托费等费用。可以看出，股票交易是一个复杂过程，将过程进行简化是必然趋势。区块链技术的运用完成了这一任务，实现了股票交易的自动化，增强了交易的安全性。

在传统的股票交易过程中，人工干预程度约为 10%。引入区块链技术之后，股票交易将实现全过程自动化，无须人工干预。通过在交易启动时引入协议，区块链能消除一些最常见的交易后出现的问题及差错，比如错误的结算指令和账户指令细节等。

如果不主动变革，就会被变革。全球各大证券交易所都已经表示出对区块链技术的兴趣，下面是全球 10 家证券交易所（排名不分先后）针对区块链技术采取的行动，如表 5-3 所示。

表 5-3　全球 10 家证券交易所针对区块链技术采取的研发行动

证券交易所	区块链研发行动
澳大利亚证券交易所（ASX）	澳大利亚证券交易所是对区块链技术最有野心的证券交易所之一。2016 年 1 月，它向区块链初创公司 Digital Asset Holdings 投资了 1 000 万美元之多，这家公司致力于为澳大利亚证券交易所提供一个可提升交易时间的区块链解决方案
芝加哥商品交易所集团（CME Group）	芝加哥商品交易所是“Post-Trade Distributed Ledger Working Group”的创始人之一，目前已通过其投资部门 CME Ventures 在行业内开展了非常积极的行动。它先后投资了分布式账目创业公司 Ripple、区块链投资集团 Digital Currency Group 以及 Digital Asset Holdings
德国法兰克福证券交易所	德国法兰克福证券交易所的运营商 Deutsche Börse 也参与了 2016 年 1 月 Digital Asset Holdings 的 6 000 万美元融资。2016 年 2 月，Deutsche Börse 表示他们正在对该技术进行相关的概念验证，尽管还没有发布任何测试结果
迪拜多种商品交易中心（DMCC）	迪拜多种商品交易中心的成员创建了 Global Blockchain Council 机构，旨在监督区块链技术应用及其发挥的影响。另外，迪拜多种商业交易中心正在与比特币创业公司 BitOasis 一起从事一项技术试验，探索区块链技术如何能够完善其人员的入职流程
日本交易所集团（JPX）	日本交易所集团是亚洲比较活跃的一个股市运营商，2016 年 2 月，它与 IBM 正式结盟，合作开发区块链应用，进行区块链实验。2016 年 4 月初，它还宣布正在和 Nomura Research Institute （NRI）合作进行试验，研究区块链技术如何被应用到证券市场。2017 年 1 月 10 日，日本金融厅已允许日本交易所集团使用金融技术，如区块链作为其核心交易基础设施
韩国证券交易所（Korea Exchange）	韩国证券交易所在 2016 年 2 月宣布将力求通过区块链技术推出一个柜台交易平台。它表示，希望区块链技术能有助于证券交易所降低成本
伦敦证券交易所（LSE）	伦敦证券交易所是追随 R3（由 40 多个银行组成的区块链联盟和区块链公司）脚步的第一大团体之一，而且它是首个表示大型金融公司可以通过合作模式进行区块链测试的公司，这超出了 R3 的框架

续表

证券交易所	区块链研发行动
纳斯达克（ASDAQ）	纳斯达克是对区块链研发最积极的机构，在2015年首次推出私人股份交易平台Linq，也因此成为第一个进行区块链概念验证的金融机构。此外，纳斯达克还与区块链解决方案提供商Chain达成了合作，并且允许其内部专家能够公开谈论区块链技术。2016年，纳斯达克透露正在和爱沙尼亚的Nasdaq OMX Tallinn Stock Exchange合作进行一项试验，以期利用区块链技术减少股东投票方面的各种障碍
纽约证券交易所（NYSE）	纽约证券交易所在2015年发布了两份重要声明，这两份声明都与比特币相关。2015年1月，纽约证券交易所投资了比特币服务公司Coinbase，成为其C轮融资的一部分。2015年5月，纽约证券交易所继续推出比特币的价格指数，这也将成为CoinDesk的比特币价格指数（BPI）的竞争者
多伦多证券交易所（TSE、TMX）	多伦多证券交易所的运营商TMX集团在2016年3月第一次公开表示出了对区块链技术的兴趣，同时，Anthony Di Iorio（以太坊的联合创始人之一）受雇为该机构第一位首席数字技术官。TMX集团还表示，它是处于生成区块链战略的早期阶段，而且它可能很快进行技术测试

区块链技术的未来充满无限可能，全球各大证券交易所已经意识到，这是千载难逢的发展机遇，所以都积极拥抱区块链。放眼未来，区块链能够掀起新的浪潮，首先将在金融业得到验证。

5.3.2 会计审计机构

比特币的核心贡献者彼得·托德（Peter Todd）认为，会计审计机构是继证券交易所之后第二类受到区块链影响的金融机构。

传统金融系统中最大的问题就是不信任。彼得·托德称："传统金融系统有一个'公开的秘密'，对于他们的数据库、员工，他们都不信任……甚至他们自己都互相不信任。因而，因为不信任而产生的问题就非常多。"

基于不信任的金融审计形成了庞大产业。彼得·托德说："银行对数据库和员工的不信任才让审计人员有了工作。为什么会有如此巨大的劳动密集型的审计基础设施以及这么多审计人员在哪里研读交易数据呢？消失的钱去了哪里？谁私自动用了钱？钱最终被转移到了哪里？这一切都是合法的吗？"

全球各大金融机构都对创建一个保存数据记录的新系统非常感兴趣，以区

块链为底层技术的比特币系统就是这样一个开放系统。如果用比特币系统取代目前的封闭账本系统，金融审计活动将会变得更加有效和透明。

紧接着，彼得·托德表示尽管金融审计产业的现状良好，但是很难再有提高。彼得·托德说："金融机构在他们的审计工作方面做得相当不错。在大多数情况下，'银行欺诈'保持在一个可接受的水平上。"

当前银行提高结算速度的瓶颈是无法解决金融活动的历史维护问题。由于审计属于劳动密集型工作，需要长达数小时的连续作战才能完成，因此很难做到即时对一致性达成共识。

那么，区块链技术则可以有效解决这个问题吗？对此，彼得·托德解释说："当前金融系统依赖于数据库管理员的信任和这个系统钥匙的持有者。从这个角度来看，一个区块链就可以充当一个强大的审计日志。"

比如，一些银行职员的工作就是简单地输入一些数据，如果他们拥有了一种绑在钥匙卡或者其他东西上的加密签名，然后以这种方式进入数据库，那么他们将会获得区块链的所有优势。其实，早在区块链获得大量关注之前，银行就已经开始探索相关技术。所以当区块链技术出现以后，银行如获至宝。

那么区块链会取代金融审计人员，让审计人员下岗吗？彼得·托德这样说道："这个问题的重点在于我们如何让区块链安全到可以取代人类的地步？"事实上，彼得·托德的答案与比特币创始人中本聪在比特币白皮书中的说法不谋而合。

中本聪在白皮书中说："我们非常需要这样一种电子支付系统，它基于密码学原理而不基于信用，使任何达成一致的双方，能够直接进行支付，从而不需要第三方中介的参与。"

2016 年 8 月，全球四大会计师事务所之一普华永道发布了他们的新区块链（PoC）概念验证的详细信息。据称，他们创建了一种实时审计流程，用于保险市场的政策制定。该项目是普华永道与智囊团 Z/Yen 的 Long Finance 项目合作进行的。他们将该项目称为"高层次政策安置流"，旨在重新定义潜在客户接受政策的方式。

在 PoC 区块链网络中，保险商、代理商和监管机构都是节点参与者。项目报告详细表示："保险商能够在区块链上浏览政策，提供报价来支撑一个特

殊政策存在的风险，而代理商则能够选择接受或者拒绝这些报价。这种在各方之间的沟通和谈判都发生在区块链中。当某个政策受到完全支持的时候，将会在区块链上创建和分享正式的保险合同。”

报告中还公布了一个项目设计图，展示了区块链概念网络中相连接的保险商、代理商和监管者节点。普华永道表示，这次概念验证测试帮助他们深入观察了区块链应用如何用于减少物理文件，简化监管报告结构以及创建一种本质上的实时审计跟踪。

在区块链应用方面，同属于全球四大会计师事务所的德勤会计师事务所采取了积极行动。德勤专门成立了一个部门，里面有 100 多个技术专家来提供区块链的各种技术服务。自 2015 年以来，德勤投入了非常大的力量研发区块链帮助他们克服各种问题的解决方案。仅仅是 2015 年，德勤在区块链解决方案方面产生的营业额就已经有了 1 个多亿美元。

普华永道、德勤对区块链新技术的态度都是积极友好的，并且已经采取了一系列研发行动。这对国内的会计师事务所的启示：应当成立区块链技术部门，争取早日让区块链参与到日常的审计工作中来，提升工作效率。

5.3.3 银行体系

本书在 3.3.2 小节中讲到，区块链的共识机制发挥作用过程中，所有的参与者共同维护数据，而不存在任何一个中心。因此，银行与银行通过使用区块链可以共享通过一个账本。事实上，银行内部也可以通过使用区块链技术降低金融系统内部监管成本。

对于银行来说，单点故障是最恐怖的事情。所谓单点故障，即由于某个节点故障造成银行内部的巨大损失。以巴林银行事件为例，一个成立了 233 年的银行，只因为一个交易员未审核便做下的一单交易，就导致巴林银行出现巨额亏损，最后不得不选择倒闭。

对银行来说，唯一的解决方法就是严格审计。因此，银行内部的监管成本非常高。2008 年金融危机之后，资金方面审核的监管成本更高了，包括反洗钱、金融反恐等都会逐渐增加监管成本。在这种情况下，更多银行突然发现，也许

区块链能解决这个问题。

所有数据可追溯、任何的单点都没有办法去篡改或者隐瞒数据，这将会降低违法行为发生的概率。可以说，如果在银行内使用区块链技术就能有效降低内部审计成本。西班牙最大的银行桑坦德银行发布的一份报告就专门谈了这个问题。

桑坦德银行认为，如果全球的金融机构使用区块链技术的话，截至2020年，每年金融机构节省的成本会超过200亿美元。所以很多人认为也许在未来的十年、二十年有很多的金融机构会使用区块链技术。

在我国，积分体系的构建与重组是银行领域比较安全的区块链技术试水区域。当前，国内银行的积分体系基本处在各银行、各业务之间互不打通的状态。总行对于各分支行的积分运营缺乏统一的协调运营，而且监管困难。很多分支行下的积分运营机制很难保证实际运营效果和客户回流情况，也难以得到精准的数据反馈。

从银行角度来说，积分体系的问题包括客户范围较小、积分业务种类较窄、积分应用项目较少等，一系列问题造成的结果是客户对银行积分的认同感偏低；从用户的角度来说，获得银行积分的成本较高、受益较小，因此用户不愿意去争取。这也使大多数用户对于银行积分体系抱有相对消极的态度。

下面以彩色币为例分析区块链如何引申到银行积分体系，解决银行积分体系的现存问题。彩色币指的是那些被“染色”或“标记”的比特币，在交易时通过备注字段来代表某种特定资产。正如在一张100元的纸币上标注文字给予某人，作为一张借据使用。这种方式可以在双方互信的基础上进行交易。

当前，银行总行和分支行之间的积分流通处于封闭环境中。引入了彩色币之后，总行负责统筹全年的积分发行总量，然后针对分支行的不同需求给积分添加信息标记，甚至在未来添加定向指令。添加上信息标记后的积分流通不影响积分在用户手中留存、转移、使用等行为，但总行可以通过积分标注对不同分支行的积分运营情况进行随时的追溯和统计。所有数据反馈都有据可依，积分情况能够精确到客户每一次的交易和转移。

彩色币积分机制解决了银行传统的多条产品线积分并行的问题。区块链是一个风险和机遇并存的新兴概念，银行应当及时对其进行研究和尝试，否则很

有可能在未来的竞争中被甩在后面。

5.3.4 大型科技企业

当证券交易所、会计审计机构、国际大型银行正在为区块链技术发烧的时候，大型科技企业也争相为金融机构提供区块链技术支持，包括微软、IBM、亚马逊、谷歌等。

2016 年 4 月，微软与 R3 区块链联盟达成战略合作协议，共同开发区块链技术。据悉，微软 Azure 云服务不仅为 R3 区块链联盟成员提供云端工具、服务以及基建，还会向其派驻项目经理、技术架构师、试验助理师和技术支持。

微软全球业务拓展执行副总裁佩吉·约翰逊（Peggy Johnson）表示："拥有智能云端技术后，R3 区块链联盟将会加快试验和学习进程，加速区块链技术的部署。"

R3 区块链联盟的 CEO 戴维·鲁特（David Rutter）说："与微软的合作将会加速区块链商业产品的落地。"戴维·鲁特还预期，外界很快就会对区块链有更深入的了解，而商业产品的开发需要 12 ～ 18 个月，而显著商业应用的但是则需要 3 ～ 5 年。R3 区块链联盟将会研发出什么样的区块链商业产品，现在还无人知晓。

早在 2014 年 11 月，微软就与纽约区块链初创公司 ConsensYs 合作推出了基于云的区块链技术平台。该平台致力于帮助金融机构高效快捷、低成本的使用区块链技术。这一平台对微软 Azure 用户是开放的，所有银行和保险行业公司都可以使用。全球四大会计师事务所普华永道、毕马威、德勤、安永已是该服务的用户。

与微软较早关注区块链不同，谷歌对区块链的关注较晚。2016 年 10 月，谷歌为苏格兰皇家银行提供云服务，帮助其进行区块链交易清算和结算。而 IBM（国际商业机器公司）、微软以及亚马逊在 2015 年就已经涉足云服务领域。

截至 2016 年年底，IBM 和微软公司已经研发出非常有效的特殊开发工具，并邀请各大银行和区块链创业公司在他们的数据中心测试新的数据库技术。作

为云服务的领头人，亚马逊也与区块链创业公司进行了合作。

2016 年 12 月 7 日，IBM 全力押注区块链，公布了一个旨在加速商业区块链应用开发的“区块链生态系统”项目。2016 年 2 月，它还推出了自有区块链 IBM Blockchain，试图在商业区块链应用行业获得更高的地位。自推出 IBM Blockchain 以后，IBM 与外界建立了多项区块链合作。而区块链生态系统项目的推出将是该公司在商业区块链领域迈出的一大步。

该区块链生态系统可以为区块链应用开发者提供指导和辅导，为区块链创业公司创造了一个应用推广平台，形成了某种意义上的“区块链应用商店”。该生态系统甚至对企业开发者和系统整合商开放。

IBM 表示：“IBM 将会提供指导和工具来减少从概念到执行阶段所需的时间。IBM 区块链专家将会通过 Hyperledger Fabric Slack 频道为开发者提供支持，以及帮助他们解决问题。”另外，该公司还会通过该生态系统提供代码库、智能合同范本以及其他工具。

从全球范围来看，区块链技术的研发尚处于初期阶段，普及率非常低，而 IBM 已经意识到了它的巨大商机。

“区块链未来的增长和普及依赖于强劲生态系统的建设。只有在创新者、行业专家和基础设施提供商携手以新的方式重塑商业交易的发生方式的情况下，商业网络才能够发生质变。”IBM 全球企业服务部高级副总裁布里奇特·范·克拉林根（Bridget Van Kralingen）指出，“Hyperledger Project 代码日渐成熟是重要里程碑。基于此，IBM 致力于提供让这些玩家能够通力合作的环境，帮助开发者加速区块链网络的建造。”

截至 2016 年年底，加入 IBM 的生态系统的创业公司已经非常多，包括鉴定追踪高价值商品和奢侈品的英国创业公司 Everledger、致力于提供云端移动技术系统的加州公司 Gliding Eagle、来自帕洛阿尔托的早期阶段基金和风投工作室 The Hive、研究利用区块链创建忠诚和奖励机制的 Loyyal、硅谷创业公司 Skuchain 等。

Block chain

第6章
区块链在物联网领域的应用

在物联网领域，区块链技术开辟了创新的无限可能性。在未来，有非常多的物联网和智能系统的区块链应用将被开发出来。区块链技术可用于追踪设备的使用历史、协调处理设备之间的交易，例如，所有的日常家居物件都会自发、自动地与外界进行金融活动。在这种环境下，家里如果安装一个智能电表，它就会自动调节用电量和频率使电费账单最优惠。现在，也许你已经想关注区块链技术对物联网到底有什么作用了，本章将详细展开相关内容。

practice

6.1 致力于物联网研究的三大区块链公司

未来十年里，区块链在物联网领域的应用将是最激动人心的。第 5 章我们提到区块链在金融领域的应用使现实世界的资产迁移到网络世界里。而在非金融领域的应用，区块链能够发挥的最大作用就是物联网。在物联网领域，各种成熟的技术公司和初创公司开始投资以及大量地研究各种区块链应用。这些应用的主要目的是连接家庭网络到云端以及周边的电子设备。下面介绍四家致力于实现物联网研究的四大区块链公司。

6.1.1 最早开发区块链的公司——IBM

IBM 是最早提出用区块链技术解决物联网现存缺陷的公司。IBM 早在 2014 年就发布了《设备民主，去中心化、自治的物联网》白皮书。白皮书展望了物联网的前景和机遇，也分析了当前物联网存在的缺陷。展望了物联网的前景和机遇，也分析了物联网想要做大亟须解决的问题。IBM 总结了物联网面临的五大挑战，内容如图 6-1 所示。

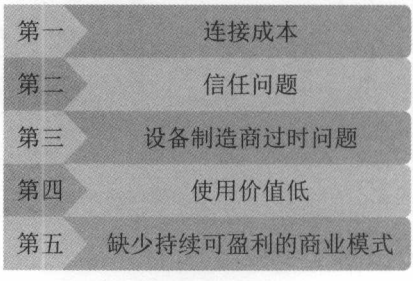


图 6-1 物联网面临的五大挑战

第一个挑战是连接成本。大多数现有的物联网解决方案成本都很高，不仅包括服务的中间人成本，还包括高额的与中心化云和大型服务器群相关的基础设施和维护成本。

第二个挑战是信任问题。物联网中的信任很难形成并维持，大多数现有的物联网解决方案总是不经过用户授权就能够收集分析用户数据，然后提供给中心化机构。物联网要想普及开来，首先需要整合隐私和匿名性，给予用户控制自己隐私的能力。

第三个挑战是设备制造商过时问题。在物联网世界，设备的生命周期总是比设备制造商的生命周期还要长。在此过程中，软件更新和设备维修成本将不断加重制造商的负担。这就导致了一种现象：设备还在使用，设备制造商已经倒闭了。

第四个挑战是使用价值低。物联网不仅仅是简单地让设备联网。大多数现有的物联网解决方案只是为了物联网而物联网，并没有产生更好的产品和服务。

第五个挑战是缺少持续可盈利的商业模式。出卖用户数据或者做针对性广告是不切实际的物联网商业模式。普通用户可能开放共享自己的数据，但是企业用户不会这样做。另外，大多数设备制造商对智能设备应用程序的收入预期太乐观，根本没有找到可持续盈利的商业模式。

在此基础上，IBM 提出，需要建立一种去中心化的物联网解决方案，实现去中心化，设备自治。而区块链技术为物联网提供了一个优雅的解决方法。

IBM 称：“运用区块链技术，可以为物联网世界提供一个引人入胜的可能性，当产品最终完成组装时，可以由制造商注册到通用的区块链里面标示着它生命周期的开始，一旦该产品售出，经销商可以把它注册到一个区域性的区块链上（社区、城市或国家），通过创建有形资产与匹配供给和需求，物联网将会创造一个新的市场。”

2015 年 1 月，IBM 宣布启动基于区块链技术的 ADEPT 研究项目。IBM 还与三星建立合作关系，专为下一代的物联网系统建立了一个概念证明型系统，探索一种不仅安全而且成本低的设备连接方式。

ADEPT 不仅应用了区块链技术，还融入了智能合约和人工智能 Waston。根据可行性报告显示，未来的家用电器可以执行一份“智能合约”来发布命令，

比如洗碗机要求洗涤剂供应商进行供货。智能合约还为设备赋予了支付订单的能力，并且能够收到零售商发出的支付确认信息和发货信息。同时，洗碗机用户将会收到通知信息。

区块链、智能合约、人工智能，三者相辅相成，将会构建出一个更强大、更智能的物联网。正如IBM全球企业咨询服务部的副总裁保罗·布罗迪（Paul Brody）所说，IBM的目标是构建一个更加智能的物联网，这个运行的设备网络能够分享能源和带宽，做决策，并能极大地提高效率。

ADEPT平台由以太坊、Telehash和BitTorrent三个要素组成。IBM和三星希望，ADEPT平台可以自动检测、自动更新、不需要任何人为操作，而且这些设备还需要与其他附近的设备通信，以便于为电池供电和节约能量。

Telehash实现了无须信任的P2P通信，Bittorrent实现了安全的分布式数据分享，而以太坊则构建了健康可拓展的设备协作方式。随着ADEPT和以太坊的影响力不断提升，区块链在物联网中烙下的印记将会越来越深。

虽然前景无限，但是ADEPT系统当前还面临很多挑战。挑战主要来自于数字货币自身的发展和稳定性，这关乎ADEPT的适用范围是否能够大范围扩展。对于稳定性问题，ADEPT团队还没有找到明确的解决方案，他们解释说：“诸如侧链、树链和迷你区块链等技术将会逐渐解决这个问题。每一种解决方式都有它的优点和缺点，但是我们还需要达成一个共识来确定一个通用的方式。”

2016年10月，IBM宣布继续推进区块链和人工智能交叉物联网项目。作为IBM布局物联网领域的另一项行动，IBM将会投资2亿美元来推动该项目在物联网领域的研究。

IBM称：“企业可以在安全、私有的区块链上来分享物联网数据，以减少成本和跨网络人力和物力的复杂性。这些功能都将完全整合到IBM的区块链中。”

作为全球科技巨头，IBM在区块链应用于物联网领域的探索将会促进区块链与物联网在世界范围内的创新发展。

6.1.2 获500万融资的公司——Filament

除了科技巨头IBM探索区块链在物联网领域的应用，另外一些公司也在

这一领域深耕，Filament 也是其中一家有名的公司，它主要从硬件基础方面挖掘着区块链在物联网领域的无限可能。

Filament 成立于 2012 年，公司最初的目标是建立网状网络上的无线家庭安全系统，后更名为 pinocc.io。2014 年 10 月，公司项目被选入 TechStars 孵化器，于是重新使用 Filament 名称，并将公司的发展目标定位于工业用例上，致力于实现设备之间的连接。

2015 年 8 月，Filament 宣布完成 A 轮融资，融资金额为 500 万，Bullpen Capital、Verizon 风投和三星风投参与了此轮融资。这是电子消费产品巨头三星的下属投资部门三星风投第一次参与投资区块链行业。在此之前，三星风投与 IBM 合作研发 ADEPT 项目，受到了外界关注。Filament 的融资状况如表 6-1 所示。

表 6-1　Filament 的融资状况

时　间	轮　次	融资金额（万美元）
2015 年 10 月	A 轮	75
2015 年 5 月	A 轮	500
2014 年 11 月	可转债券	52.5
2014 年 10 月	种子轮	2
2014 年 2 月	风险资金	5
2013 年 8 月	种子轮	100
2013 年 2 月	众筹	10.5

完成 A 轮融资后，Filament 宣称通信协议 Jabber/XMPP 的发明者杰里米·米勒（Jeremie Miller）已经受邀成为公司 CTO。1999 年推出的 Jabber 通信协议是美国在线即时信使（AOL Instant Messenger）等聊天应用的开放标准替代物，最终被 Facebook、谷歌以及微软公司在不同程度上采用。此举意味着 Filament 决定复制 Jabber 通信协议的成功。

Filament 的联合创始人兼首席执行官艾瑞克·詹宁斯（Eric Jennings）解释说：“Jabber 通信协议的成功给我们的启示是去中心化系统对于使用它的公司和用户来说更有价值。这是我们从中学到的精神，更为宝贵的是，这种去中心化的系统可以实现用户之间的平等地位。”

Filament 的理论建立在找到一个可以用来实现设备连接的去中心化平台基

础之上。艾瑞克·詹宁斯说："去中心化系统对与之互动的人更有价值……这点是需要注意到。那我们为什么使用区块链呢？因为区块链使系统更强大，更有价值。"

基于这一设想，Filament 的项目与 ADEPT 项目在本质上非常相像。不同的是，ADEPT 项目致力于实现家庭自动化，而 Filament 的项目将针对工业市场，使石油、天然气、制造业和农业等行业的大公司实现效率上的新突破。

试想一下，工业设备一般都分布在一个辽阔的范围内或者部署的地方非常偏远，甚至没有手机信号，比如铁路网络，石油管线和电网等。要想使这些设备加入物联网，最大的问题就是信号传输。另外，当用户通过网络对物联网中的设备进行操作时，所有操作过程和数据都会记录在互联网日志上。随着操作数量的增加，服务器的存储能力和运算能力必须越来越高，这就导致实现物联网的成本非常高。

Filament 是如何解决这两个问题的呢？基于区块链技术，Filament 开发了一套能把现有的工业基础设备通过远程无线网络沟通起来的技术。这种远程无线网络的用途非常广泛，既可以用来追踪自动售货机里面的存货情况、检测铁轨的损耗情况，还可以帮助农场主管理自家的农场。

在这种远程无线网络技术的基础之上，Filament 推出了 Filament Tap 和 Filament Patch 两个传感器设备。

Filament Tap 是一种便携式连接设备，内部嵌有的传感器可以检测周边环境，然后连接到设备上开始监控。Filament Tap 还实现了无线网络的快速部署，与周边 10 英里以内的节点（其他 Filament Tap 设备）通信，并可以使用手机、平板电脑和计算机进行沟通。Filament Patch 与 Filament Tap 配套，是用来延伸该技术的硬件，可以实现硬件项目的定制。

Filament Tap 设备与邻近 10 英里远的设备通信现在正处于测试阶段。一旦测试成功，Filament Tap 将被用于监视电力设施，可以降低物理检查电力设施的成本。如果发生 Filament Tap 设备着火或者其他意外状况，互联互通的其他设备也可以向电力公司发出提醒。

此外，Filament 还试图利用比特币构建一个供电网络，这是可以实现的。区块链将在安全、透明度和大数据管理方面改善物联网，而 Filament 公司希

望从底层硬件出发，为区块链在物联网领域的应用探索做出贡献。

6.1.3　开发物联网支付方案的物付宝——Tilepay

物付宝（Tilepay）对物联网的探索集中在支付领域和商业模式上。物付宝的目标基于区块链技术，为当前的物联网行业提供一种人到机器或者机器到机器的支付解决方案，实现对物联设备传感器的实时接入支付。

物付宝还开发了一个基于比特币区块链技术的微支付平台 SPV（Simplfied Payment Verification）。作为一个去中心化的支付系统，SPV 能够被下载并安装到任意一台个人电脑上、平板或者手机上。物付宝的设想是，所有的物联网设备都会有一个独一无二的密码，通过区块链技术接收支付。物付宝还会构建一个物联网数据交易市场，人们可以在里面购买物联网中各种设备和传感器上的数据，并以 P2P 的方式保证数据和支付的安全传输。

物付宝看到了物联网未被挖掘的潜在价值，即传感器数据。物联网之父凯文·艾什顿（Kevin Ashton）先生说过：“物联网的价值不在于采集数据，而在于数据共享。”

世界上的数据是海量的，但是人们并不擅长采集数据。遍布全世界的传感器网络因此诞生，不仅成本非常低，还与互联网相连。计算机便是利用这些自动化的传感设备获取信息的，然而，我们构建传感器网络的真正目的是通过采集数据的物联网得到整体的图景。

传感器采集到数据以后，数据是否发挥应有价值在于信息能否共享。尽管传感器铺设是物联网的架构基础，但是现有的大部分传感器都被私有网络掌控，只为有限的应用服务。这种现状根本不是物联网的初衷——数据共享。

举例来说，大型商场为了检测停车位的使用情况，花费大量的金钱安装了一个大型的传感器网络。对于任何公司来说，构建这样的基础设施都是必要的，但是成本非常高。最终，巨资建设的基础设施只能用于判断停车位情况，实在是可惜。其实，商场完全可以将其中的数据资源提供给研究人员作为参考。

还有一些重视科技应用的水务公司在水龙头上安装传感器，这些传感器上关于洗手频率的数据对一些卫生组织制定政策具有参考价值，但由于这些数据

只属于这家公司，卫生组织也无可奈何。

可见，上述物联网中的数据并没有掌握在需要该数据的人手中。一方面，拥有物联网数据的公司们没有意识到市场对物联网数据的渴求；另一方面，物联网根本不存在一个有利于分享与交易的商业模式。尽管 Xively、Thingspeak、Thingful 等云平台支持个人分享传感器数据，但是由于缺乏对数据拥有者的奖励机制，使数据拥有着不愿意提供持续稳定的元数据。

所以，建立一个物联网的全球数据市场进行数据分享交易是必要的。2014 年，两位瑞士的学者发表了论文《如何通过比特币交换传感器数据并实现传感器自盈利》，其中就提到了直接向传感器支付费用获得数据信息的设想：建立一个由传感器端、请求端、传感器库组成的系统，处于这个系统中的传感器可将其测量数据值上传至世界范围的数据市场中，利用比特币区块链进行数据交易。

物付宝正在做的就是整合全球传感器数据，让设备实现自盈利，建立起传感器之间去中心化的“支付宝”。想象一下，如果物付宝研究成功，每个传感器都可以进行数据交易，那么一个私有的停车场管理公司下属的停车场传感器，可以通过物付宝搭建的平台实时出售当前停车数据，研究人员可以通过应用程序购买它的当前数据用作研究。

当然，现实面临的挑战还有很多。由于物联网技术非常复杂，上下游产业链较长，再加上区块链的发展还处于早期阶段，走向真正的物联网世界还有很长的路要走。但现在，物付宝已经整合了物联网与区块链技术的相关厂家，共同开发并着手制定了相关产业标准。

在软件开发领域，物付宝与 ignite 软件开发公司展开合作，专注于区块链和智能合约软件的开发；在物联网传感器领域，物付宝与汇集了全球无数物联网传感器实时数据的 Thingful.net 网站深度合作，使传感器节点支持物付宝的协议和功能；在硬件产业链上，物付宝和 6.1.2 节讲述的 Filament 公司合作开发区块链网络，使 Filament 公司的所有开源硬件都可以加入到物付宝的网络里面。此外，Tilepay 还与硬件制造商 Cryptotronix、ATMEL 以及智能穿戴设备开发商 nymi 合作，为物联网领域带来基于比特币区块链的硬件小微支付方案。

为了实现设备自盈利，物付宝在物联网领域不断探索，踩出了一个又一个

坚实的脚印。当区块链与物联网联合，两者将会实现优势互补，为人类带来更智能的生活。

6.2 还未实现万物互联的物联网

物联网是一个非常广泛的概念，涵盖了所有的领域。从全球范围内来看，无论是 IBM 早期所提的“智慧地球”还是思科倡导的“万物互联”，或者是新加坡要构建的全球首个“智慧国”等，都属于物联网。自 2009 年概念期过后，物联网已经逐渐导入成长期，随后进入高速发展期。然而，当今的物联网，还没有实现真正的万物互联。

6.2.1 物联网原理

物联网（Internet of things）的意思是物物相连的互联网。如果物联网时代来临，人们的日常生活将会发生翻天覆地的变化。

根据市场调研机构 IDC 发布的最新报告，到 2020 年，全球物联网市场规模将从 2014 年的 6 558 亿美元扩大到 1.7 万亿美元，全球存在于物联网内的终端设备也将从 2014 年的 1 030 万个增至 2 950 万以上。还有机构预计，到 2020 年，中国物联网市场规模将达到 10 万亿元人民币。

大多数人对于物联网的概念都是懵懵懂懂的，下面我们一起看看物联网的原理。物联网是在计算机互联网的基础上构建的，主要利用射频识别（RFID）、无线数据通信等技术，达到万物互联的结果。在物联网构建的网络里，所有的物品都可以自发进行“交流沟通”，无须人的干预。这种“交流沟通”的实质是利用射频自动识别技术实现物品自动识别和信息的互联与共享。

在物联网构想中，射频识别技术是让所有物品发起“交流沟通”的一种技术。射频识别标签中存储着规范且具有互用性的信息，无线数据通信网络可以

将这些信息自动采集到中央信息系统实现物品识别，进而通过开放的网络进行信息交换和共享，从而实现物联网的终极目标——万物互联。

6.2.2 物联网的技术架构

6.2.1 小节讲到物联网的原理，下面接着看看物联网的技术架构。物联网架构分为三大层次，内容如图 6-2 所示。

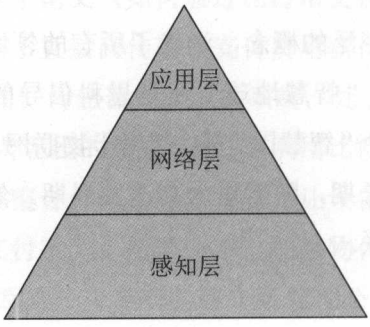


图 6-2 物联网架构三大层次

作为一个系统网络，物联网与其他网络一样都有内部独有的架构。物联网的系统架构分为感知层、网络层、应用层三层。感知层主要是利用射频识别、传感器、二维码等技术达到随时随地收集物体信息的目的；网络层主要通过融合各种电信网络与互联网使物体信息快速而准确地传递出去；应用层是将感知层收集的物体信息进行处理，最终用于智能化识别、定位、跟踪、监控和管理等实际应用中。

在物联网的技术架构中，传感器技术、射频识别标签以及嵌入式系统技术是三大关键技术。

传感器技术是物联网应用中最关键的技术，也是计算机应用中的关键技术。众所周知，几乎所有的计算机都只能处理数字信号，所以自计算机诞生以来，就需要传感器把模拟信号转换成数字信号，然后交给计算机处理。

射频识别标签也属于一种传感器技术，因为射频识别技术是融合了无线射频技术和嵌入式技术为一体的综合性技术。在自动识别、物品物流管理等领域，

射频识别技术都有着广阔的应用前景。

嵌入式系统技术是一种复杂的技术，因为它融合了计算机软硬件、传感器技术、集成电路技术、电子应用技术等多项技术。嵌入式系统技术的应用已经有几十年之久，小到人们身边的 MP3，大到航天航空的卫星系统，无不是嵌入式系统技术的应用。那些具有嵌入式系统特征的大大小小的智能终端正在改变着人们的生活，推动着工业生产以及国防工业的发展。

如果把物联网比作人体，传感器就是人的脸、眼睛、鼻子、嘴巴等感官，网络就是用来传递信息的神经系统，而嵌入式系统则相当于人的大脑，在接收到感官传来的信息后要进行分类处理。这一形象比喻将传感器、嵌入式系统在物联网中的位置与作用形容得非常贴切。

总而言之，物联网是基于互联网将用户端延伸和扩展到了任何物品与任何物品之间，然后进行物品间信息交换和通信的一种网络概念。

6.2.3　物联网开启爆发式增长大门

2016 年 11 月 30 日至 11 月 1 日，世界物联网博览会在江苏无锡举行。参加会议的政府有关负责人和权威专家都认为，经过前期发展积累，物联网已经迎来了非常多的机遇，很有可能就此开启爆发式增长大门。

物联网迎来的机遇有四重，内容如图 6-3 所示。

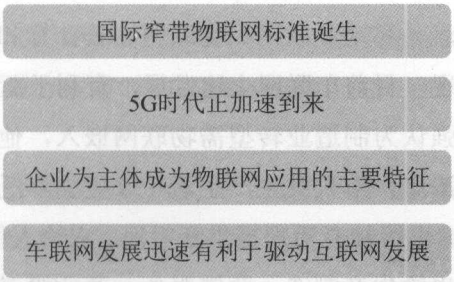


图 6-3　物联网迎来的四重机遇

第一重机遇是国际窄带物联网标准诞生。物联网曾经发展困难，主要原因是 60% 以上的低速率传感器应用匹配不到合适的传输手段。由于传输距离短、

覆盖窄，使用光纤与移动通信成本高，但是 WiFi、蓝牙连接又不可靠。2016 年 6 月，窄带物联网标准 NB-IoT 在韩国釜山获得通过，这意味着物联网这一“瓶颈”得到化解。

窄带物联网的特点有四个：一是覆盖广，覆盖能力是当前的移动通信的 100 倍之多，穿透力可达到地下车库；二是连接大，支持的终端数是传统移动通信的 50 ～ 100 倍；三是功耗低，一个电池就能支持一个物联网模块工作长达 10 年；四是成本低，1 美元是芯片成本的最终目标。

第二重机遇是 5G 时代正加速到来。对物联网来说，高速网络是必需的。在 2020 年之前，5G 技术很可能将会逐步成熟并投入试运行。如果 5G 时代来临，一平方公里支持一百万个物联网终端将不是问题，这对于扩展物联网应用，促进物联网和移动互联网深度融合有重要意义。

第三重机遇是企业为主体成为物联网应用的主要特征。截至 2016 年年底，包括三星在内的很多大企业都进入到物联网领域。从 2017 年开始，三星的电子设备都要变成物联网上的设备。

对国内外众多大企业来说，物联网是新的业务增长点。在国内，华为、联想、中兴、中国电科、神州数码以及三大电信运营商等都将智慧城市作为集团的主要战略方向，而智慧城市是以物联网为基础的。在国外，谷歌耗费 32 亿美元收购了一家烟雾传感器企业，宣布正式进军物联网领域。

第四重机遇是车联网发展迅速有利于驱动物联网发展。事实上，汽车就是物联网的节点，物联网正在给汽车重新下定义。一辆好汽车上可以有上百个传感器，自动驾驶汽车就是移动互联网、物联网、云计算和大数据技术与先进汽车技术融合的最佳体现。目前车联网火速发展，有利于驱动物联网发展。

江苏省委书记李强认为制造业转型需物联网嵌入，他说：“物联网将以其颠覆性变革、全面性渗透，给人类生产生活带来更加广泛而深刻的影响。它给经济发展植入新基因，也给社会治理提供新手段；它给人们衣食住行乃至教育、医疗带来极大便利，也给生产制造、营销服务、商业模式带来颠覆创新；它给物理世界的万事万物带来结构性的时空重塑，也给人们的理念、思维和行为方式带来深刻变革。”

李强还表示：“改革开放以来，江苏经济经历了两次大的转型，第一次是

发展乡镇企业，实现了由农到工的转变；第二次是发展开放型经济，实现了由内到外的转变。现在正在进行第三次转型。物联网是这次转型的优先选项，也是一个重大战略选择。”

我国当前还处在经济转型的关键期，传统制造业必须向更高端发展。而物联网发展迎来的机遇同样也是我国经济转型期的机遇。抓好这一机遇，既可以加速制造业向智能制造的转型，也能引爆物联网产业的增长。

6.3 区块链 + 物联网

除了金融业以外，物联网算得上是与区块链联系最密切的领域了。如果将区块链技术应用于物联网，将可以保证这个终端数量庞大的设备网络高效运行，不仅能提高系统速度，节省一些复杂的环节，还能增强其真实性。

6.3.1 传统中心化模式的超高维护成本

当物联网普及之后，这样的场景可以实现：冰箱里的牛奶不多了，冰箱可以自动联系供应商下订单，执行自助服务进行维护，通过外部资源下载新的制冷程序，合理安排时间周期降低电力成本，与对等设备协商优化环境；汽车可以通过智能操作找到最方便省时的路线，还能让主人在路过的商店顺便购买一包香烟……

所有的情景都将会通过物联网实现。很多不利用计算机的行业已经被大量的联网设备代替了，尤其是其他技术（比如区块链）与物联网相结合时会有更多这样的事情发生。

但是，物联网遇到的主要问题是难以实现设备之间以及设备与设备所有者之间的互动。在当前物联网系统无法解决这一问题时，技术公司和研究者希望通过区块链技术解决这些问题。

在没有遇到区块链之前，物联网生态体系只能依赖中心化的代理通信模式或者服务器 / 用户模式。在这个生态体系里，所有的设备都通过云服务器验证连接在一起，设备之间的连接仅仅通过互联网即可实现，尽管只是在几米的范围里。而这个云服务器要求具有非常强大的运行和存储能力。

这种物联网模式连接通用计算机设备已经有几十年了，而且依然支持着小规模物联网网络的运行。尽管如此，随着物联网生态体系的需求不断增长，云服务器已经满足不了巨大的需求。众所周知，当前的物联网解决方案是非常昂贵的，因为中心化的云服务器、大型服务器以及网络设备等基础设施的维护成本都非常高。当物联网设备的数量需要增加至数百亿甚至数千亿时，海量的通信信息产生了，这将会极大地增加成本，使物联网中心化模式遭遇“瓶颈”。

即使成本问题和工程问题都能顺利解决，云服务器本身依然是一个“瓶颈”和故障点，这个故障点有可能会颠覆整个网络。从物联网的当前环境看，云服务器的这种颠覆性作用还没有明显表现出来，但是当人们的健康和生命对物联网的依赖越发明显时，这就显得尤为重要了。

因为我们无法构建一个连接所有设备的单一平台，也无法保证不同厂商提供的云服务是可以互通而且相互匹配的。而且设备间多元化的所有权和配套的云服务基础设施将会使机对机通信变得异常困难。

区块链技术破解了物联网的超高维护成本以及云服务器带来的发展“瓶颈”。区块链可以通过数字货币验证参与者的节点，同时安全的将交易加入到账本中。交易由网络上全部节点验证确认，消除了中央服务器的作用，自然就不需要为维护中央服务器而付出超高成本。

6.3.2 区块链让物联网真正实现去中心化

区块链与物联网的结合可以构建一个物联网网络去中心化的解决方案，从而规避很多问题。采用标准化 P2P 通信模式处理设备间的大量交易信息可以将计算和存储需求分散到物联网网络中存在的各个设备中，这样可以避免网络中任何单一节点失败导致整个网络崩溃的情况发生。然而建立 P2P 通信的挑战非常多，最大的挑战就是安全问题。

物联网安全不仅仅是保护隐私数据这么简单，还需要提供一些交易验证和达成共识的方法，防止电子欺骗和盗窃。那么区块链带来的解决方案是什么呢？

区块链为 P2P 通信平台问题提供的解决方案是一种允许创建交易分布式数字账本的技术，这个账本由网络中所有的节点共享，而不是交给一个中央服务器存储。

区块链分布式账本是防篡改的，恶意犯罪分子根本没有机会操纵数据。这是因为分布式账本不存在任何单点定位，也没有可以被截断的单线程通信，有效避免了中间商攻击。区块链真正意义上实现了可信任 P2P 的消息传送，并且已经通过以比特币为首的数字货币证明了自己在金融业的价值，不利用第三方中介就可以完成 P2P 支付服务。

将区块链用于物联网也存在一些挑战，比如处理能力和能源消耗就是一个需要考虑的问题。区块链交易加密和验证时需要计算密集型操作，这要求有大量的算力才能执行完成，而很多物联网设备缺乏的就是算力。存储方面也存在一些问题，因为账本记录的信息将会越来越多，这就使网络节点中存储的账本记录也越来越多。

市场研究公司 Machina Research 的分析家吉米·格林（Jeremy Green）解释说："由区块链驱动的自治物联网网络将会给制造商寻找的商业模式带来挑战，这种商业模式包括有持续收入来源的长期订阅关系。因此，制造商们必须做好心理准备，区块链将会彻底颠覆当前以及预期中的商业和经济模式。"

现在，区块链技术的应用还处于初期探索阶段，但是可以预见，物联网和区块链的结合是前途无量的，去中心化自治网络会对物联网的未来起决定性作用。

6.3.3　左手比特币，右手物联网经济

冰箱、汽车、医疗器械和许多其他设备，有一天都将会与互联网相连。进一步来说，在物联网下，这些设备之间可以彼此通信和交易，这是比特币的一个潜在应用。未来的物联网经济，或许是以比特币为基础的物联网经济。

对于物联网研究者来说，物联网就是一个系统，这个系统可以将世界上任何一个物理对象都变成一台接入到互联网的计算机。当研究物联网经济（物联网运行的商业模式）时，我们应该可以想到每一个物理对象将变成一个在全球数据市场里自主运行的数据与钱进行交换。

比如，一个停车场管理公司安装了一个全国性的传感器网络来检测停车位的使用状况。对于停车场管理公司来说，基础设施的构建耗费了大量的金钱，但是这些信息可以帮助停车场管理公司回收一部分成本。当用户开车四处寻找停车位时，可以通过一个应用程序查看从 20 几个传感器实时传送过来的车位信息，并为此支付费用。

那么，用户以什么方式来支付费用呢？首先停车场管理公司作为传感器提供者需要与服务提供者签订一份协议。用户如果需要使用停车场管理公司收集来的数据，必须要向服务者提供购买服务，或者用自己的个人数据来交换停车场管理公司的数据。

现在，有另外一种简单的方法可以帮助用户完成数据交易。此时，比特币就能发挥作用了。使用比特币完成数据交易的实质是通过比特币向提供数据信息的传感器直接支付费用。

比特币具有开放性，对于任何人和任何事物，包括每一个传感器。所以，每一个传感器都可以有自己的比特币账户，免费而且不需要任何人为介入。那么，一个数据集信息价值多少呢？可能连一分钱都不到。尽管很多人都怀疑传统的支付系统是否有能力高效地管理比特币，但是已经有很多比特币开发者正在致力于研发使用比特币进行小额的交易支付。

基于比特币的物联网经济是一个巨大的机会，Bitnet 比特币支付平台的 CEO 约翰·麦科唐纳（John McDonnell）说：“物联网之下，机器都可以相互交谈，完成支付。一台喷墨打印机的墨水快要用完的时候，可以自动向惠普订购打印机墨水。”

约翰·麦科唐纳所谈到的场景是物联网经济的关键。现在，如果办公室里打印机的墨水用完了，但是你急需打印一些文件，那么只能说你运气不好。物联网经济下就不存在这个问题，如果打印机意识到墨水将要用完的时候，它可及时联系打印机公司，然后订购更多的墨水，你甚至没有注意到这些事情是什

么时候发生的。而这一切的前提是打印机可以使用比特币进行支付。

如果用户仍然需要对打印机有所控制，那么打印机可以连接到用户的手机。当墨水即将用完的时候，打印机会发送短信给用户，让用户知道打印机里墨水的状态以及它的订购计划，然后经过用户批准后再执行交易。

比特币让这所有的一切有了实现的可能。就像 Stripe 数字货币部负责人克里斯蒂安·安德森（Christian Anderson）所说的：“我们拥有了这种开放的技术基础，就很容易在这之上建立一些东西，比如物联网。”

Block chain

第7章
区块链在大数据领域的应用

当我们在比特币的范围内讨论区块链的时候，区块链貌似与大数据关系不大。但是在比特币之外的金融贸易、商业合同、股票交易等领域，区块链与大数据有很大关系。以金融贸易领域为例，巨大的区块数据集合包含着每一笔金融交易的全部历史，这些数据通过分析可以得到另外一些价值。然而，区块链提供的完整性数据，并不能进行分析，所以这时候就涉及大数据以及其分析工具。

practice

7.1 大数据分析价值创造模式

从发现价值到创造价值，大数据已经成为了“互联网 +” 产业升级的动力源。在过去，数据主要在决策领域发挥价值，即通过数据收集、管理、分析等方法将数据转化为价值进而提供决策支持，比如商业智能在企业管理层面上的应用。随着数据的体量增长以及数据处理能力的提升，大数据已经成为一种有价值的资产，不仅可以用于决策支持，还能发挥创造价值的功能，例如，完善个人征信体系、提供实时交通信息服务等。

7.1.1 什么是大数据

大数据不是简单意义上的大量数据，而是涵盖了数据处理与分析能力以及为人发现价值、创造价值的新概念。IDC 的一项研究显示，未来 10 年里，全球的数据量将会以每年 40% 的速度增长。到 2020 年的时候，全球数据量将达到 35ZB，大数据将迎来 ZB 时代。

这还没有结束，未来的数据量最终会达到什么级别是我们难以想象的。大数据中“大”的定义一直在刷新。在 2003 年左右，1GB 数据已经算得上是大数据；10 年后，1 000GB 数据也还好，并不是非常大；如今，ZB 级别的数据也不会令人诧异。事实上，大数据的核心也不是“大”，而是价值。大数据的本质就是数据，没有足够有效的分析与应用，再大的数据都没有价值。

大数据包含很多类型的资料，不仅包括传统意义上有行有列有数值或者文字的数据表单，还有视频、声音、图片、文档等。传统数据表单是一种结构化数据，其余的数据被称为“非结构化数据”。结构化与非结构化数据每时每刻

都在成倍地增加。比如，全上海道路上的视频监控，摄像头多达十万个，全天候地记录着图片与视频，一旦发生交通意外情况，这些数据就成为处理问题的重要资料。

几十年以后，利用视频数据搜索到一张特定身影或者脸孔将成为非常简单的事情。但是，视频类大数据应用还需要数据分析技术来实现。同样，基于声音、图片或者文本的分析与数据挖掘将为人类理解大数据带来革命性的突破。尽管大数据的实际应用还很少，但大数据很快便会火爆起来。

人们对大数据的印象似乎就是数字、图表、图形等，并没有什么真实体验到的感觉。实际上，通过数字、图表形式进行基本的数据处理、分析与预测，是大数据应用的初级阶段，这个阶段的数据应用是很难被用户具切实感受到的。

随着大数据在实际场景中的应用落地，人们将会在日常生活中的各个场景中感受到以大数据为基础构建出一个更真实、更智能可控的世界。当大数据完全渗透进人们的生活，与大数据相关的生活应用也会越来越多，场景化的呈现模式也将应运而生，同时也会催生出更多的可能性。

随着大数据场景化应用的不断深化，人们不仅能够领略到航空领域的大数据，还将感知并体验到多维度的大数据应用。比如，用户出行的天气数据、地面交通等实时数据。当这些数据进行了场景化应用后，就会出现以下情形。

一家公司的业务经理预计今天出差回来，其助理要去机场接机。助理为了保证顺利接机，避免因天气或者堵车延误了接机时间，他打开一个大数据的场景化 APP 随时随地查看实时的天气与地面交通动态以及实时航班动态信息。如此一来，助理合理安排了接机行程，避免了偶然情况的发生。

在具体的商业场景和产业生产中，大数据才能发挥其重要价值和意义。“得数据者得用户”“得数据者得天下”的说法是片面的，因为大数据本身的价值并不大，只有将其运用到实际场景中，大数据本身才产生了价值。所以，企业应该建立数据库，将之转化为有价值的数据财富应用到产业化场景中，强化企业核心竞争力，建筑企业竞争壁垒。

企业对大数据的应用包括收集、积累、处理、应用等一系列环节，而数据价值体现在产业化的管理和使用环节中。企业应当正确看待大数据的价值与作

用，将大数据作为产业链中必不可少的驱动力与创新力，使其发挥“内核发动机”的作用。大数据的产业化应用可以促进人类经济社会生产与再生产，实现产品与服务的最优化。以下是大数据产业化应用的三个主要层面，内容如图 7-1 所示。

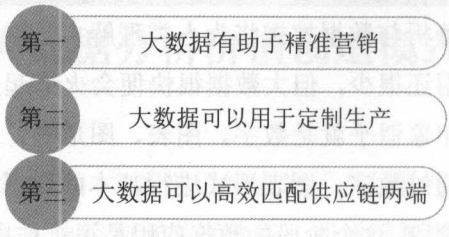


图 7-1　大数据产业化应用的三个主要层面

第一，大数据有助于精准营销。企业根据市场需求进行生产，然而却总是出现生产过剩或者商品滞销等问题。根本原因是产品或服务与消费者之间有“一堵墙”，也就是说，产品或服务与消费者之间缺乏近距离沟通。大数据对目标消费群体多维度的特征描述可以帮助企业推翻产品或服务与消费者之间的“墙”。

互联网时代，各种大数据手段能够捕捉到用户的个人数据以及网络行为数据，并通过数据化处理手段将其保留在云端。而且用户每一次在互联网上出现都能被监测到，并将用户产生的数据不断累积最终形成精准的用户画像。企业通过大数据对用户的定位可以实现精准营销，促进利润增长。

第二，大数据可以用于定制生产。定制生产是以消费人群的细分为基础进行产品设计、生产，以满足日益丰富的多层次、个性化的消费需求的生产模式。随着消费者市场的形成，企业必须看重细分领域消费者的需求，通过提供更个性化的产品与服务提升企业竞争力。

实行定制生产对企业提出了严苛的要求，企业必须在产品设计、生产、供应、销售以及配送等各个环节上适应小批量、多样式、多规格的生产和销售变化。在定制生产过程中，大数据在挖掘消费者个性需求、产品设计、建立多渠道营销策略等方面起着重要的参考和促进作用。定制生产的所有环节的出发点都是消费者数据。

电商与传统企业追求的最高境界是一样的，都希望做成个性化、一对一定制生产的经营模式。在市场竞争日渐激烈的情况下，定制生产将成为企业获得市场有利地位的有效途径，而大数据的价值在定制生产时代将发挥得淋漓尽致。

“（Consumer to Business，C2B）消费者到企业”和“大数据”的互联网概念给众多企业管理人带来了关于企业生产模式的新思考。很多业内人士认为，基于互联网大数据开展的定制服务逐渐成熟，即将开启产品销售的新模式。早在2012年，海尔开展网上投票的活动，让消费者定制自己喜欢的电视。随后苏宁、国美等电器企业也开始进行定制家电营销。

天猫电器也推出了 C2B 家电定制生产模式。定制生产模式共包括 12 条小家电生产线，可以生产 12 款“定制小家电”产品。定制模式推出的一天时间内，电烤箱、吸尘器、扫地机、电风扇等电器销量共达到 18 万台。突出的销售业绩引来业界的广泛关注。天猫此次营销活动以多年以来收集的消费者大数据为基础，并也获得了美的、苏泊尔、九阳等十余家家电企业的大力支持。

定制生产的产品，将会得到市场的接受认可，并在很大程度上受到消费者偏爱。定制生产的理念促进了企业资源配置的最优化，避免了定位不精准导致的产能过剩。其中，检验数据的可靠性与可挖掘价值以及是否应当将其看作定制化生产指标的问题至关重要。这样一来，企业就必须注重收集数据的科学性、逻辑性与准确性。

第三，大数据可以高效匹配供应链两端。精准营销和定制生产是从企业端和消费者端来讲的。企业端对消费者端的精准营销和消费者端对企业端的定制模式是大数据产业化应用最广泛的场景。实际上，大数据在企业与消费者之间充当了信息桥梁的角色。

企业与消费者的沟通经常出现问题，比如，企业市场定位的偏差，消费者传达的伪需求等。一旦两者出现沟通失误，企业的产业链将变得冗长和落后，致使成本费用增高，效率低下，而且消费呈萎靡、滞缓的状态。而大数据能够真实地体现一个企业的状况，一个消费者的状况，然后告诉企业消费者想要什么样的产品，告诉消费者不同企业产品与服务的差异之处。

企业和消费者是产业链的两端，双方反馈速度的快慢都由中间环节的长短

决定。产业链过长将导致双方反应速度滞后，而市场经济环境变幻莫测，供应与需求之间的及时匹配本就很难保证。因此，企业应当建立产业生态链条的全闭合和高效供需匹配机制，做到实时响应、反馈，寻找企业与消费者的利益契合点并且进行组合搭配。

大数据的挖掘成本和价值含量，直接影响着企业的未来发展。大数据存在的意义就是应用，大数据高层级的产业化应用是当下数据发展的方向。数据产业化是一个市场机遇，而中国正在经历着数据时代的变迁，企业应当抓住这个千载难逢的机遇。

7.1.2 一切都以数据为依据

如今，电商、汽车、手机、化工等几乎所有行业都在开展以大数据分析为基础的各种应用，比如：电商通过用户行为数据的分析，以达到促销和相关货品推荐的目的；航空公司通过旅客反馈数据分析，以改进空中服务；汽车厂商通过客户维修信息数据的分析，以改进汽车硬件的可靠性增加客户的满意度；手机公司通过手机销售量预测数据分析，以优化库存，降低成本。

一切都以数据为依据的互联网时代，已经昂首阔步的向人们走来。随着产业化的变迁，大数据的应用价值逐渐成为企业的利器，使企业在市场竞争中占据先机，所向披靡。Facebook 就是一家致力于大数据应用的公司之一。

Faceboo 创始人马克·扎克伯格（Mark Zuckerberg）曾透露，不希望用户通过“踩”（dislike）按钮去表达反对意见。不过，Facebook 已经计划公开测试的新按钮将帮助用户表达更多样化的情绪。例如，当用户看到让人心痛的内容时，用户可以通过一些踩按钮去表达自己的同情情绪。扎克伯格表示，“用户对‘踩’按钮的要求已经有很多年了，我们将开发出满足更大规模用户群需求的产品。”

Facebook是美国一个提供社交网络服务的网站，单日用户数已经突破十亿。其创始人是马克·扎克伯格。扎克伯格的团队一直致力于对用户行为数据的研究分析，从而达到发送针对性广告的目的。用户行为包括点赞、分享、评论以及点击页面情况等。在互联网时代，各大互联网巨头拥有海量用户数据信息是

不可争辩的事实，Facebook 赖以生存的基础就是用户的情绪数据。

大家知道 Facebook 是怎么利用大数据的吗？ Facebook 甚至知道用户什么时候跟别人约会，什么时候跟恋人分手。Facebook 在其公开博客中宣称，利用用户的情绪数据，Facebook 可以判断用户是否恋爱、何时开始恋爱、何时跟别人约会以及何时分手。也就是说，Facebook 可能还比某些情侣更早地就察觉到了他们之间萌生了爱意。

无论是传统的线下情侣交往，还是社交网络中的用户确立恋爱关系的过程都会经历“求爱”的阶段。美国研究员卡洛斯·迪乌克（Carlos Diuk）认为，“沿着时间的推移，社交网络中的用户在求爱期发帖会明显增多。而一旦确立了恋爱关系，两人在对方 Facebook 留言板上发的帖子都会减少。因为热恋期的情侣总愿意花更多时间在现实生活中相处”。

Facebook 通过对大量用户情绪数据进行分析，得出这样一个结论：用户在成为情侣之前的 100 天里，即将坠入情网的两人相互发帖数量越来越频繁。而两人正式确立情侣关系后，相互发帖数量越来越少。相恋的两人发帖数量的最高峰在正式确立情侣关系之前的 12 天里，平均每天发帖数为 1.67；而确立情侣关系以后的 10 天里，两人平均每人每天发帖数为 1.53。

出现这个现象的原因与迪乌克的描述相符，情侣在度过求爱期以后，双方共处的时间增加，线上互动自然就少了。迪乌克表示，Facebook 的用户数据还显示了另外一个有趣的现象，即用户在告别单身之后，情侣之间的互动充满了爱意，互动内容越来越甜蜜。

Facebook 非常喜欢利用用户的情绪数据玩转数据分析。2012 年的时候，Facebook 就开始收集用户主动公开感情的数据对数据分析做出尝试。当时，Facebook 通过让用户分享自己的收听习惯已经积累了大量用户收听音乐的习惯数据。拥有八卦心的 Facebook 团队将情感关系和音乐这两个概念巧妙地融合在一起开始了数据挖掘工作。

最终，Facebook 找到了用户进入一段恋爱关系后喜欢收听的歌曲以及分手后喜欢播放的歌曲。2012 年情人节当天，Facebook 发表了一个有趣的歌曲排行榜，取得了很好的传播效果。Facebook 将分析结果用在基于数据的推荐引擎上，给了用户更优质的用户体验。Facebook 还利用各种数据分析的推测

结果建立了新的社交服务功能——向用户提供最契合心境的曲目。

Facebook 对用户情绪数据的价值挖掘获得了成功。不久之后，Facebook 还将采用一项全新的监测手段，不仅能够准确地收集每个用户的行为数据，还能预测用户行为背后的情绪信息。这些新的数据将丰富 Facebook 长期积累收集的海量数据。

Facebook 的分析主管 Ken Rudin 表示这项方案目前还在试验中，不会大面积推广。由此收集到的数据是否可靠而有价值还无法下定论。未来，Facebook 一旦发现这项监测手段的好处并对所有用户实施监测，所面临的用户隐私方面的问题将亟待解决。对此，Facebook 保证说："我们绝不会向 Facebook 以外的任何人分享用户的情绪数据，也不打算通过它来收取高额广告费。"

《华尔街日报》相关报道称，Facebook 正在开发对用户行为的监测的方案在目前的互联网行业中没有出现过，而普遍流行的监测方式是通过开源的 Hadoop 框架进行用户数据分析。相关数据表明，Facebook 在最近的几年里已经收集分析了超过 300PB（1PB 等于 1 024TB，1TB 等于 1 024GB）的数据信息。

将海量数据收集整理分析的作用是企业不仅可以利用最好的技术获益，还可以利用最好的信息获益。为了进步发展，企业必须在信息技术方面投入大量金钱和精力。Facebook 对大数据的运用还给了其他企业一些启示，内容如图 7-2 所示。

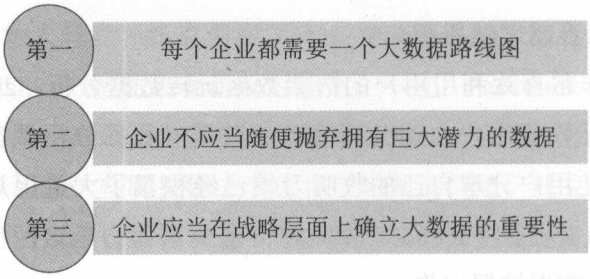


图 7-2　Facebook 对大数据的运用给了其他企业的启示

第一，每个企业都需要一个大数据路线图。在高速增长的信息时代里，每个企业都需要一个大数据路线图。美国产业分析研究公司福雷斯特（Forrester）估计，企业数据的总量每年增长将近一倍。每个企业都应该制定获取数据的战

略，包括企业内部计算机系统的常规机器日志以及线上用户的交互记录。即使企业并不知道这些数据的意义，也必须收集这些数据。数据的价值在偶然的情况下就可能显现出来。

第二，企业不应当随便抛弃拥有巨大潜力的数据。企业还需要一个计划以应对数据的指数型增长。照片、即时信息以及电子邮件的数量非常庞大，由手机、GPS 及计算机构成的“感应器”释放出的数据量更加无法估量。企业应该建立相应的数据收集、管理系统以应对暴增的信息数据。

第三，企业应当在战略层面上确立大数据的重要性。GE（通用电气公司）的全球战略与文化就是六西格玛及相应的数据分析流程。不仅如此，GE 坚持不懈地推动以数据分析为基础的持续改善工作。GE 还在高端航空发动机研发以及能源系统业务领域方面，导入了代表数据分析界最高水平的实验设计（DOE）方法，对进一步提升其研发水平起了很大作用。

任何企业都应该像 GE 一样，具备一种将数据分析贯穿于整个组织的视野。通过观察谷歌、亚马逊、Facebook 和其他科技领袖企业，我们发现了大数据带来的无限可能性。管理人员需要做的就是在组织中融入大数据战略。

国外大型互联网巨头们应用大数据进行决策已经数年有余，他们在大数据应用方面已经获得了广泛的成功。尽管我们很难达到相同的水平，但是学习他们的成功经验，一定可以促进企业的自身发展。

7.1.3　以萧山警匪案为例看大数据分析的价值

大数据通过解读个体和用户从而产生价值，企业可以运用大数据解析目标用户来促进销售和获得盈利，政府部门也可以利用大数据分析提高工作效率。下面要说的就是大数据分析应用于政府职能部门的案例。

政府部门运用大数据的例子非常多。比如，通过大数据分析掌握舆情，实现舆情预判和引导，最终提升政府部门的监管能力；政府部门还可以利用大数据侦查案件，打击违法犯罪。2016 年 5 月 31 日发生的杭州萧山“5 • 31”北干山命案告破就充分证明了大数据的价值。

案情回顾：2016 年 5 月 30 日上午，一对母女（母亲 25 岁，女儿 5 岁）

在杭州市萧山区北干山游玩后失踪，萧山警方接到报警后派出10多只警犬和20多名训导员连夜在山上搜寻。循着几滴血迹，警犬最终在北干山一厕所旁找到了嫌疑人留下的血衣和刀鞘。

5月31日凌晨，警方找到了母女两人的遗体，但是凶手不知所踪。接下来的几天里，大规模的警犬连续搜寻北干山，把北干山来回走了一遍，最终确定嫌疑人已经离开山上。

凭借着大数据分析寻找线索以及严密的“网格化”防控模式，萧山警方最终于6月5日晚将犯罪嫌疑人抓获归案，杭州萧山“5·31”北干山命案最终成功告破。在不到一周的时间里，大数据是如何帮助萧山警方成功破案的呢？大数据分析对萧山警方破案的帮助如图7-3所示。

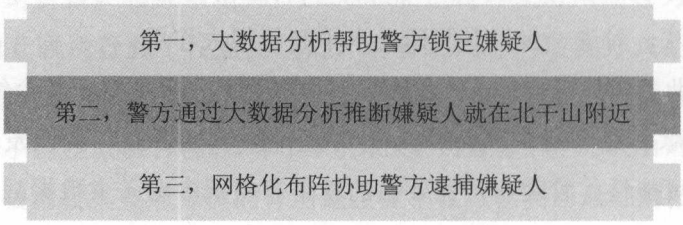


图7-3　大数据分析对萧山警方破案的帮助

第一，大数据分析帮助警方锁定嫌疑人。负责现场勘验的民警在一处隐藏于密林中的厕所里发现了血迹，并在附近发现了掉落的男鞋和鞋垫。通过现场勘验情况及外围调查，警方确定掉落的鞋子和鞋垫正是嫌疑人的。随后，警方利用大数据对血迹以及鞋子进行鉴定和分析，锁定了一名36岁的安徽籍男子有作案嫌疑。

第二，警方通过大数据分析推断嫌疑人就在北干山附近。锁定嫌疑人后，警方的视频作战团队同步上线，300多名视频操控员随案跟进，展开大数据分析。自2010年以来，萧山区新增添了近万个监控点，很多都是高清探头，为警方破案提供了非常好的条件。最重要的是，警方监控团队已经建立了一套成熟的大数据分析机制，可以最大限度地追踪对象，获得追踪对象尽可能多的行踪信息。

根据监控大数据分析的结果，警方成功获知了嫌疑人案发前一天的行踪。

2016 年 5 月 30 日上午，嫌疑人从杭州城区乘坐公交车进入萧山区，最后从萧山区博物馆附近上北干山，直至案发。结合监控分析与现场勘验的结果，警方推断，嫌疑人已经受伤，就躲在北干山附近。

第三，网格化布阵协助警方逮捕嫌疑人。紧接着，警方出动了公安路面交警、特警、治安等警力，围绕北干山周边布置卡点与警力，让民警把守城区主要出入口，一张大网就此形成。

另外，警方还发出网格化巡查指令，要求网格员积极行动，进一步搜寻嫌疑人可能落脚的地方。在北干辖区，有一个特殊群体，他们包括了社区干部、公交司机、商店店员、环卫工人，他们不仅活跃在街头路面，还活跃在各自网格的微信“望望群”里，随时准备给警方提供嫌疑人线索。

最终一名药店员工在 2016 年 6 月 5 日的傍晚发现一名可疑男子在店外徘徊多次后进店买了一盒止痛药，然后匆匆离去。药店员工很快就向网格民警打电话通报，随后，警方在中誉网格附近的一草丛中发现并逮捕了嫌疑人。

这一案件充分体现了大数据分析对案件侦破的价值。互联网以及大数据分析将是未来政府职能部门提升核心竞争力的关键。

除此之外，大数据分析还可以在企业市场推广中发挥纠察功能。对警方来说，大数据分析可以有助于他们分析预判罪犯信息并锁定罪犯行踪；对企业来说，大数据分析同样可以帮助他们在市场推广中找到作假数据，识别真假用户。

说到造假，渠道刷量造假已经不是什么稀罕事，而且互联网 APP、游戏 APP 、直播 APP 等都是被严重爆刷的目标。这意味着企业白白投入了大量的推广成本却没有成效。从传统视角来讲，企业根本不会辨别真假用户数据，但是从大数据的视角来看，问题就比较容易解决。下面一起来看大数据分析判读真假用户数据的原理。

首先，通过留存率做基础判断。留存率是多数企业判断渠道质量的标准。一般情况下，留存率分为次日留存率、2 日留存率、3 日留存率、周留存率、14 日留存率、月留存率等指标。如果用户数据是真实的，那么留存曲线就会是一条平滑的指数衰减曲线，基本没有突然增长或者突然下降的异常波动。留存率下滑指数曲线如图 7-4 所示。

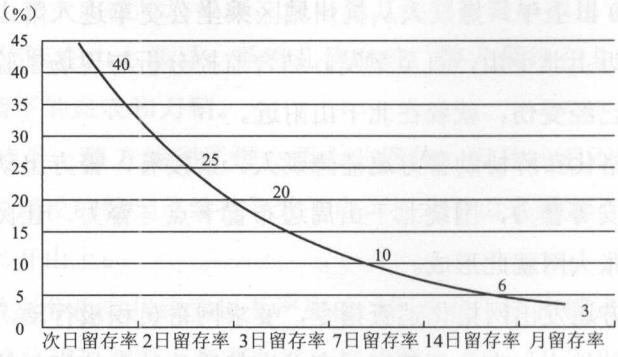


图 7-4　留存率下滑指数曲线

如果出现了异常波动，包括明显断层、留存清零等现象，说明渠道通过积分墙等方法干预了数据。这样的用户没有质量可言，也不具有商业价值。

其次，结合转化率、平均启动数据以及用户在应用内的行为数据进一步判断。随着机刷行为的智能化，通过留存率下滑指数曲线图可能发现了问题。此时，我们要怎么来判断甄别真假用户数据呢？

一是结合转化率来做判断。一般情况下，注册转化率应当高于次日留存率。因为用户首先完成注册，第二天打开 APP 的意愿才更大一点。如果用户连注册的意愿都没有，第二天打开 APP 的意愿一般非常小。这样说来，如果出现次日留存率高于转化率的情况，那么用户数据很可能是假的。

二是结合平均启动数据做判断。一般情况下，用户每天打开 APP 的次数也是呈指数下滑趋势的，如图 7-5 所示。

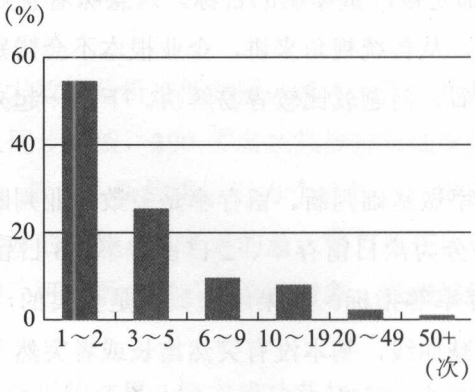


图 7-5　日启动次数分布

如果渠道用户大部分每天都是只打开 1 ～ 2 次 APP，那么渠道用户数据很可能是造假的，建议立刻停止投放。

三是结合用户在应用内的行为数据来判断。遇到一些技术高超的造假刷量公司，上述的数据指标也可能判断不出什么，这就需要对比分析渠道用户在应用内行为数据与整体用户行为数据，包括访问页面、使用时长、访问间隔、互动频率等行为数据指标。大多数 APP 刷量机器人仅仅能够模拟出看似真实的用户行为，但是与真实的用户行为数据还是无法保持一致的。

四是，观察长期表现后再做判断。短期数据的真假难以判断，但是长期数据就比较容易，比如月留存。综合对比之下，很容易看出渠道数据的真假。另外，各行各业中都会有一些平均水平的数据指标，我们大可以参考这些指标评判渠道质量的好坏。总之，利用大数据分析判断市场推广数据的真假是一个非常有效的方法。

2016 年，李克强总理多次在大数据论坛峰会中致辞，倡导政府与企业关注并运用大数据。大数据所显现出的价值已经印证了一句话：“未来最大的能源不是石油而是大数据”，可以想象，大数据将是未来政府与企业提高竞争力的突破口。

7.2 区块链上的大数据更具有可信性

一般认为，数据发展经过三个阶段。在第一阶段，数据是无序的，而且没有经过充分检验；在第二阶段，大数据兴起，通过人工智能算法进行质量排序；在第三阶段，数据采用区块链机制获得基于互联网全局可信的质量。正是区块链能够让数据进入第三阶段。可以说，区块链上的大数据是人类目前获得的信用最坚固的数据，其精度和质量都非常高。

7.2.1 区块链与大数据共建未来信用

区块链出现的重要历史原因就是对信用的需求日益增长。商品经济最初的

方式是物物交换，但是这种交易方式成本很高，主要是运输成本。在这种情况下，市场经济开始考虑降低交易成本，于是很快就过渡到了利用信用建立交易的方式。信用建立是金融的核心，而传统的信用建立大多依赖“中心”，包括央行、商业银行、法院等。

传统金融的信用成本也比较高，主要是金融基础设施建设成本。比如，一些人喜欢在城市周边骑自行车郊游，对于不喜欢随身携带现金的人来说，他们可能会遭遇无法住店、不能吃饭，甚至连水都买不到的情况。

后来，市场上又出现了互联网金融。以微信为例，通过大数据来建立信用是其主要特征。互联网金融的基础是大数据金融，大数据使信用建立的成本比传统银行吸储放贷方式的成本降低了很多。随后出现的一系列互联网金融行为都出现信用建立成本下降的趋势。

那么，区块链与大数据结合在一起有必要吗？众所周知，互联网解决了信息的自由传递问题，但是资产不可以。在现实环境中，资产在传递过程中具有所有权唯一，不能随便复制的特点。所以，第一代互联网 TCP/IP 协议无法使人们在互联网上建立所有权和信用制度。

作为比特币的创始人，中本聪认为信用建立不能依赖某个中心，因为任何过度中心化的结果都会产生信息不对称的问题，会存在利用中心权力损害参与者的利益、损害市场上其他方利益的情况。因此，比特币白皮书开篇就提出：“我们要开创一种不需要第三方的、不需要中介的支付系统，电子货币的支付系统。”

中本聪倡导的不依赖任何中心的信用构建方案就是我们所说的区块链技术。区块链系统中完成的每笔交易都盖了“时间戳”，防止重复支付等问题。如果有人重复支付，那么时间就会产生矛盾，系统会自动识别为非法交易。根据一定的利益规则，矿工受利益驱动负责为每一笔交易盖“时间戳”。矿工的利益是每 10 分钟全网只能竞争到的唯一的合法记账权的奖励。谁竞争到了，就可以获得一定数量比特币的奖励。同时，全网其他矿工要同步一致它这个记账，然后竞争下一个区块记账权。

区块链通过全网作证重新构建了信用体系，这种方式仅仅以计算资源为代价。当人们已经开始讨论下一代微信以及下一个阿里巴巴时，他们还没有意识到，下一代最有可能就是一个真正去中心化的系统。

到时候，用户在任何 APP 上产生的数据都可以通过加密算法保存在区块链上。用户自己掌握着私钥，可以使用这些数据。当用户需要向银行贷款时，只要向银行提供自己的公钥和私钥，银行就能分析区块链上系统上的大数据，得出贷款人的信用情况。在未来，我们每个人都会通过区块链系统上的大数据获得全球信用。

如果说传统金融的信用建立在钢筋水泥的大厦之上，那么未来信用将建立在区块链上的大数据上。看看我们现在的信用生活：如果没有政府的认证，出生证、结婚证以及房产证都是没有人承认的。当我们出国的时候，更是会遇到各种各样的麻烦，比如合同得不到承认或者无法执行等。当前的信用执行系统成本非常高，包括法院、警察等，而高昂的成本都由我们每个人分摊了。

在未来，区块链上的大数据会为我们公证。比如，公证你和女儿的母女关系，这将会在几分钟里成为区块链上的数据，全网公开。如果有人想要篡改你们的关系，除非他能够控制全网超过 50% 以上的算力。

在区块链大数据时代，未来的信用依赖全网公证实现，这是极具颠覆性意义的。每个消费者将依靠区块链上的大数据获得信用，而区块链会成为全球金融的基础架构。

7.2.2　区块链是验证数据出处和精确性的核心工具

区块链技术的复杂性以及普及率低影响了其应用推广，然而我们无法否认它的巨大潜力，因此只能强调其巨大潜力来吸引开发者的关注。

2016 年 5 月，IDC 发布相关报告，称区块链是验证数据出处和精确性的核心工具，可以用于数据升级追踪，帮助不同数据领域建立起真正的权威数据。

IDC Government Insights 的研究主管肖恩 • 麦卡锡（Shawn McCarthy）表示：“当前，政府对 IT 安全、信息安全和可靠性表现出了极大的重视。而区块链技术是 IT 经理人的强大工具，在数据安全领域作用重大。政府可以利用区块链技术减少欺诈、提高安全性，搭建和公民之间的新关系。”

根据 IDC 的报告，区块链是改善数据真实性和精确性的基础。因为区块链可以转移和监控代表有价物品的不同实体，在审计跟踪方面可以发挥稳定作

用。区块链主要利用共享记录来跟踪实体活动，这保证其不受到黑客攻击以及未授权更改的影响。如果通过 P2P 网络建立了共享的权威数据版本，众多节点会共同工作以保证数据的完整性。

区块链的共识协议负责检查活动的有效性以及是否可以添加到区块链上。审核通过后，区块链会将这个权威记录与其他信息核对。联邦数据融合中心非常适合使用这种方法收集反恐情报。

区块链在数字货币、财产登记、智能合约等领域的应用是毋庸置疑的，但是 IDC 该项报告关注了区块链的另外一些特点。

第一个特点是数据权威性。区块链为数据赋予的权威性不仅说明了数据出处，还规定了数据所有权以及最终数据版本的位置。第二个特点是数据精确性。精确性是区块链上数据的关键特性，意味着任意对象的数据值记录都是正确的，形式与内容都与描述对象一致，可以代表正确的价值。第三个特点是数据访问控制。区块链可以分别跟踪公共和私人信息，包括数据本身的详细信息、数据对应的交易以及拥有数据更新信息的人。

肖恩·麦卡锡总结说：“我们建议企业和政府机构把区块链解决方案的机遇和价值研究纳入第三平台战略，可以通过内部战略文件确定区块链的意义以及应该遵循怎样的实施路径”。

目前，已经有政府机构开始测试区块链解决方案的数据保护和权威性管理能力。区块链有希望在大数据领域发挥验证数据出处和精确性的关键作用。

7.3 区块链可解决数据所有权问题

所有的参与主体共同创造了海量数据，尤其是在腾讯 QQ、微信这样的社交软件上，但每一个参与主体得到大数据的所有权了吗？参与主体能够掌控自己的大数据吗？答案是否定的。区块链为解决数据所有权错配问题提供了可能性。

7.3.1　数据所有权本应由数据生产者享有

2016 年 1 月 9 日，发生了一个非常恶劣的事件——“百度卖吧”事件。在百度形成的每一个“吧”包含的所有数据以及资源的所有权应该归属于用户，就连“吧主”也是由参与用户选举产生的。然而，百度居然将产生效益的吧数据公开出售，这是用户难以接受的。

在舆论的压力下，百度最终于 1 月 12 日对外宣称：“百度贴吧所有病种类吧全面停止商业合作，只对权威公益组织开放。”

同样，我们每天在微信上产生的数据有多少？人们每天产生的社交、交易数据本应该是完全属于产生者每一个人的。依据互联网共享、平等、透明的精神，这种大数据应当是一种“全球性的信用资源”。

自从人类发明了记录工具，比如文字、纸张和硬盘，数据就在不断地产生。在以前，人们并不关注数据所有权，因为数据很少会被当作商品参与市场交易（私下或非法付费交易不算）。互联网的发展使数据的价值越来越高，数据商品化趋势明显，因此数据所有权问题凸显出来。

作为商品，数据与无形资产的特征相似，可以无限复制而没有损耗。而且，数据的所有权、许可使用以及收益和转让也都有法律保障。一般认为，无形财产的初始所有权与财产的生成及价值起源相关联。

比如，文学作品的版权首先属于创作作品的作家，因为作品之所以产生价值是因为作家付出了劳动。即便素材一样，不同的作家来创作，作品的内容风格也各不相同。这说明，作品中蕴含了作家的思想人格，所以现代法律将无形财产的初始所有权视作创作果实，肯定了作者的人格和创造性劳动的价值。在这一点上，数据与其他无形财产却显得不一样了。

众所周知，数据的价值并不是来自记录者。数据只有准确反映被记录主体的身份、性格、行为习惯等信息才具有价值。只有忠实于被记录主体，准确反映后者的身份性格行为习惯等，才具有价值。不论是用户的浏览记录、消费者的行为数据，还是公司营运数据，一旦脱离了被记录的人、事、物，数据便毫无意义与价值。

由此可见，数据的全部价值来自于被记录主体。因此，根据上述无形财产

的一般原理，数据的价值产生与初始所有权统一，那么数据所有权的归属者应当是被记录主体。这也符合人类的认知。

比如，无论是谁记录同样一套数据，数据内容丝毫不会改变。因为就数据的价值来说，谁来记录或者用什么工具记录并没有什么关系，重要的是记录的是谁。当然，数据的采集整理离不开记录者和记录工具以及投资人的支持，但是投资和采集整理产生的是次生权利，根本不能动摇数据的初始所有权。

综上所述，数据从属于被记录主体，是数据产生价值的关键所在。而记录者及其工具手段与数据内容的关系则是松散可以置换的，而不是数据价值的起源。因此，数据的初始财产权应当属于被记录主体。

区块链的诞生保证了数据生产者的数据所有权。对于数据生产者来说，区块链可以记录并保存有价值的数据资产，而且这将受到全网认可，使得数据来源以及所有权变得透明、可追溯。

一方面，区块链能防止中介拷贝用户数据的情况发生，有利于可信任的数据资产交易环境形成。数据与传统意义上的商品有很大不同，具有所有权不清晰、可以复制等特征，这也决定了中介中心有条件、有能力复制和保存所有流经的数据，这事实上侵犯了数据生产者的数据所有权。这种情况是无法凭借承诺消除的，也构成了数据流通的巨大障碍。当大数据遇上区块链，数据生产者的数据将得到保护，中介中心无法拷贝数据。

另一方面，区块链为数据提供了可追溯路径。在区块链上，各个区块上的交易信息串联起来就形成了完整的交易明细账单，每笔交易的来龙去脉非常清晰，如果人们对某个区块上的数据有疑问，可以回溯历史交易记录判断该数据是否正确，对该数据的真假进行识别。

当数据在区块链上活跃起来，大数据也将随之活跃起来。

7.3.2 区块链破除大数据孤岛效应

尽管所有的互联网公司都倡导公开、透明、共享的互联网精神，但事实上，他们根本不会将手中的大数据与其他公司共享。在当前形势下，大数据必然是每一个公司的绝对内部资源，不可能进行无边界的共享，这就出现了“大数据

集中”的问题。

在这种情况下，互联网的发展存在一个悖论，与其初衷大不相同。集中的大数据引起了马太效应，即富者愈富、穷者愈穷。在大数据孤岛的作用下，大数据资源集中在少数人手中，全社会的数据资源不能流动，只有少数的掌控者才能使用这些宝贵的数据资源。作为大数据的生产者，用户个人根本无法获得信用资源的主动权，这非常不利于全球市场信用成本的进一步下降。

区块链与大数据技术的结合有望打破大数据孤岛的局面，这主要是因为区块链的实质是一个分布式账本。基于这个分布式账本，区块链可以保证投票选举是公正公平的。因为区块链可以记录任何交易，而投票选举也是一定意义上的交易，所以区块链可以记录下来谁投票给了谁、选举过程是怎样的等。根据区块链上的数据，我们可以知道这次投票选举是否公平、公正。

对于区块链创业公司来说，致力于为企业、行业提供解决方案是没有问题的，但是解决方案是否能够真正落地还是一个未知数。可以说，区块链技术当前的发展状况就相当于 90 年代的互联网技术，它对行业发展以及政府、企业运行方式上的改变是一定会发生的。可以预见，2020 年左右，全球将会出现上百甚至上千个区块链联盟。

区块链是一种通过去中心化和去信任的方式集体维护一个可靠数据库的技术方案，这也注定了区块链与大数据联系在一起是必然的。甚至可以说，区块链的诞生是对大数据的重构。

7.3.3　Enigma项目助用户售卖数据

麻省理工学院（MIT）的研究生 Guy Zyskind 研发了一个区块链项目，并得到了创业家 Oz Nathan 和麻省理工学院著名教授亚历克斯·彭特兰（Alex Pentland） 的帮助。该项目名为 Enigma，将会为云数据共享带来空前的灵活度——帮助公司分析客户的数据，并且保证客户的隐私信息安全，并在不共享数据的前提下允许贷款申请人提交自动承保信息。

用户甚至可以通过 Enigma 项目在市场上售卖大型计算与统计的加密数据，而且不必担心数据泄露以及通过互联网落到未知人手里。团队还称，此项目会

在不久的将来推出一个 beta 测试。

Enigma 项目团队在白皮书中写道："当隐私安全以及自动控制得以保证，安全措施增加后，用户可以销售自己的数据地址。例如，想要寻求临床试验的病人的药剂公司可以检索基因数据库。市场可以为客户收购消除摩擦，降低成本，并提供新的收入流。"

Enigma 项目使用了安全多方计算密码技术，数据分往不同的服务器，因此没有机器可以提取完整的基本信息，但是节点仍然可以获得共同计算数据的授权功能。他们可以在不泄露信息的情况下将功能传送到其他节点。团队在白皮书中指出："没有任何团体能够拿到整体数据，也就是说，任何一个团体都只能获得毫无意义的一部分数据。"

对于公司来说，Enigma 可以用来储存客户的行为数据和信息，利用许可系统让职员们或合伙人分析大量记录，而且还没有数据泄露的风险。银行也可以根据计算标识贷款承保原则在用户提供的加密数据基础上执行自动脚本，而申请者永远也不会共享他们的财产细节数据。

Guy Zyskind 强调："用户可以贷款、储蓄加密货币或者购买投资产品，这些都由区块链自动控制，没有任何公开财产情况的风险。"

7.4 区块链助力大数据预测市场

大数据能够预测未来！事物的发展变化都是有规律的，大数据分析可以发现这种规律，洞察先机。比如，阿里巴巴的电商平台每天产生数亿交易额，用户们通过搜索寻找自己心仪的产品，而大量用户搜索的关键词就被阿里巴巴记录在了数据库里。阿里巴巴通过数据分析，能够发现当前热销产品，预测即将火爆的产品，并根据分析结果针对性的投放广告，提升转化率。对于大数据预测市场，区块链能够发挥什么作用呢？

7.4.1　Augur预测市场项目已众筹60万美元

大数据应用于预测市场的道理很简单，而区块链在预测市场方面又存在哪些潜力呢？线上众筹平台 Augur 洞察先机，首先发现了区块链对大数据调研、分析、咨询以及预测市场的撼动作用，称会提供一种类似于普通博彩的服务。

首先，一起看看什么是预测市场。与股票市场有一些相似之处，比如两者都支持用户买卖股票。不同的是，股票市场是对一个公司的未来价值进行投机，而预测市场是通过对未来事件结果的可能性判断做出购买决定。

例如，一个预测市场可能问“杰布 • 布什（Jeb Bush）会在 2016 年能被选为美国总统吗？”如果“不会”（No）股票的价格是 0.58 美元，可以理解杰布 • 布什落选的可能性是 58%。大量的经济和学术研究发现，当预测市场因为货币的参与有了足够的流动性和交易量时，预测市场就是世界上最精确的预测工具之一。

接下来，我们再来看看什么是 Augur。Augur 是以太坊平台上的去中心化预测市场平台。任何人都可以使用 Augur 为自己感兴趣的话题创建一个预测市场，比如谁会当选美国下一届总统，并提供初始流动性，这是一个去中心化的过程。作为回报，该预测市场的创建者可以从市场中获得一半的交易费用。

预测市场的交易流程是这样的：普通用户通过自己掌握的信息进行判断，并在 Augur 上预测、买卖符合自己判断的股票，例如，杰布 • 布什不会当选美国总统。当事件发生以后，如果你预测正确，持有的股票是正确的结果，那么你的股票每股将会升至 1 美元，而你的收益就是 1 美元与你当初的买入成本之差。如果你预测错误、持有的股票是错误的结果，那么你不仅不会获得奖励，买入成本还会全部亏损。

Augur 提供的服务是完全去中心化的，其宗旨是“超越体育博彩，开创新的预测市场”。用户可以使用这项服务在不同的地点对体育赛事和股票下注，还可以对选举结果、自然灾害等其他的事件下注。

与传统的预测市场相比，Augur 在很多方面都是不同的，而最重要的区别就是 Augur 通过区块链做到了全球化和去中心化。全球任何区域里的任何人都可以使用 Augur ，这为 Augur 带来了前所未有的流动性、交易量以及传统交

易所无法想象的多种视角和话题。

截至2016年年初，Augur完成了面向全球的众筹，最终筹集到价值超过520万美元的比特币。Augur将以太坊作为基础技术，如果最终获得成功，将会进一步巩固以太坊在区块链行业中的地位。

截至2017年年初，Augur已经正式进入测试阶段，并开始向首批用户开放。据知情人士介绍，Augur拥有高级前端设计，而且其市场开发形式超越了简单“是或否”二进制。

乔伊·库克（Joey Krug）是Augur的联合创始人以及核心技术开发人员，他说：“我们会把Beta测试版本作为Augur正式发布前的迭代测试平台。它包含三个阶段：第一阶段是功能有限的买卖单系统；第二阶段是加入共识机制和事件结果解决的支持机制；最后阶段进行正式REP测试。”

什么是REP呢？REP是Augur系统发行的代币。信誉代币就像比特币一样可以分割和交易，是一种与个人的公、私地址相关的“积分”。如果说比特币与黄金的性质类似，那么信誉代币就是信誉的模拟品。

Augur的实践结果报告机制引入了REP代币，具有去中心化特征。在传统的中心化预测市场，中心化的人或组织是事件结果的确定者，而Augur采用的去中心化的事件结果报告机制却不一样。每当事件发生以后，众多REP代币持有者对事件结果进行报告，而普通用户无须持有REP代币就可以在Augur上进行预测、交易。

在Augur应用之初，持有REP代币的人每八周就会对系统中随机选择的到期事件进行预测结果报告。持有者需要从三个选项里选择一个：一是事件发生；二是事件没有发生；三是模糊不清。如果持有者认为预测结果模糊不清，可以将报告推迟到下一期公布。在事情没有决议之前，持有者有两周时间来做报告。Augur的开发者希望这一过程能够十分快速地进行，预计等Augur普及之后，这一过程有可能在一小时内完成。

在两周的投票期内，如果REP代币持有者没有按照规定报告指派给他们的事件结果或者报告不诚实，主成分分析法（PCA）会把这些不负责任的持有者的信誉重新分配给那些经常做报告并且信誉良好的持有者。要想从投票过程中获得交易费用，REP代币持有者必须做到诚实。

7.4.2　普林斯顿大学聚焦比特币交易预测市场

通过上一小节的学习，我们知道预测市场是一个纯粹的投机市场。创建预测市场的唯一目的是做各种商业预测，从业务预测到现实世界里的天气以及各种真实发生的事件预测。由计算机科学家 Arvind Narayanan 领导的普林斯顿大学的一组教学人员就正在开发基于比特币交易的预测市场。

包括谷歌、英特尔、GE、西门子在内的一些巨头公司通过不同的预测市场技术获得竞争优势，但事实上，金融界一般不鼓励创建预测市场。预测市场的最大问题是它支持纯粹的投机行为，而一些地区的监管机构认为这就是赌博。比如，全球最大的预测市场 Intrade 就因为美国商品期货交易委员会断言它是一个赌博的违法方式而被迫关闭。

随后，Intrade 开始研究一个新版本的市场，并表示不会使用硬币进行交易。这或许就是由计算机科学家 Arvind Narayanan 领导的普林斯顿团队正在研究用比特币代替硬币进行预测市场交易的原因。由于比特币不是法定货币，受到的管制较少，可以使预测市场受到尽可能少的金融监管。

Arvind Narayanan 表示：“既然我们拥有比特币这个出色的分散系统，可以让双方在没有中央权威的前提下进行交易，那我们就一定可以让仲裁事件以某种形式被分散。”

爱尔兰一家预测市场机构 Predictious 创建于 2013 年 7 月，虽然相对不知名，但仅仅半年内就已经完成了 30 万美元的业务量。

比特币开发者迈克·赫恩警告说，由于比特币的竞争对手是 PayPal 和信用卡，所以比特币注将渡过一个艰难时期。但是比特币很有可能在利基产业立足，包括预测市场。

Block chain

第8章
区块链在医疗领域的应用

除了金融领域、物联网领域以外，医疗领域也是区块链技术的重要应用场景。区块链在医疗领域主要有四大应用，分别是区块链电子病历、DNA钱包、药品防伪、蛋白质折叠。本章详述区块链在医疗领域的四大应用。

practice

8.1 区块链电子病历

区块链电子病历是区块链在医疗领域内最主要的应用。区块链电子病历是利用区块链对个人医疗记录进行保存，无论是看病还是做健康规划，都有了历史医疗数据可以进行查询。而且区块链电子病历的真正掌握者不是某个医院或第三方机构，而是患者自己。

8.1.1 查询历史医疗数据

对患者来说，每一次去新的医院看病时，都需要重新录入全部的病例信息，这对患者来说是一个非常麻烦的事情。如果历史医疗数据有误，结果将更加严重。比如，之前的病例记录中血型信息或过敏数据是不正确的，那么患者在下一次接受治疗时很有可能造成非常严重的后果。对医疗机构来说，患者的历史医疗数据不齐全也不利于对患者的病情做出最精准的判断。

区块链电子病历是实现医疗信息数据共享的最佳解决方案。如果区块链电子病历得以实施，所有的常见病例、既往病例都有着清晰明确的记录。医生给病人制订诊疗方案时，可以参考有效、连续的诊疗记录，提高治病效率。比如，医生询问你对哪些药物过敏，但是你自己都不知道。如果用区块链系统存储个人医疗记录，这个问题就变得很简单，医生只要将你的病史资料调出来看就知道了。

下面一起来看四家研究区块链电子病历的公司。Healthnautica 是一个医疗记录和服务方案供应商，2000 年成立，总部位于芝加哥。Healthnautica 具有一个可定制化的客户驱动的云软件系统供医生操作和患者办理手续，使医院、

医生和病人之间的沟通更为流畅。

Healthnautica 开发的 eORders 产品在很大程度上提升了手术治疗以及程序调度过程，使网络延迟的现象减少，而且还解决了数据莫名丢失的问题。

Healthnautica 的合作方 Factom 是美国著名的区块链公司，专门提供区块链技术服务，利用区块链技术开发各种应用程序，包括医疗信息记录、审计系统、投票系统、供应链管理、法律应用、财产契据以及金融系统等。

Factom 将维护区块链数据网络视为自己的使命，帮助政府部门以及商业社会简化数据记录管理、记录商业活动，并解决数据记录安全性和监管性的问题。这在一定程度上降低了管理真实记录、进行独立审计以及遵守政府监管条例的成本和难度。

2015 年 4 月，Healthnautica 与 Factom 联合发表声明，宣称将会建立合作，共同研究运用区块链技术保护医疗记录以及追踪账目，为医疗记录公司提供防篡改数据管理。

Healthnautica 的客户，包括医院、医生以及患者都希望通过运用 Factom 的不可变更账本来对医疗记录和合约进行验证和时间标记，从而提高效率并确保医疗数据记录的安全性。

Healthnautica 发言人声称：“我们非常愿意将 Factom 的技术运用到医疗健康产业，我们开发软件与 Factom 有相同的目的，就是在既保证医疗数据的完整性的同时又保护病人隐私数据。对合作研究记录防篡改以及保存和数据追踪，我们双方都感到十分地兴奋。”

Healthnautica 的董事长 Shailesh Bhobe 说：“Factom 的技术特别适合于审计跟踪以及我们保存的客户医疗记录。”其董事会成员 Andrew Yashchuk 说：“我们的下一步动作是推动保险公司运用区块链技术保存数据，因而各方能够验证合约有效性并提升医疗账单支付效率。”

HealthNautica 与 Factom 的合作是区块链技术在医疗健康领域的第一次商业化运作，开启了区块链在医疗数据保护领域的新篇章。

Gem 是一家致力于构建全球医疗保健综合体并为人们提供更加私人化和性价比更高的服务的区块链企业。Gem Health 是 Gem 旗下一个应用开发网络并且能够向医疗保健服务商提供网络基础设施。目前，Gem Health 探索的区

块链应用包括：健康网络、药品供应链、医疗数据存储、理赔、通用健康身份以及基因数据管理等。

2016 年 5 月 11 日，Gem 宣布完成 710 万美元的 A 轮融资。关于 Gem Health，Gem 的创始人兼 CEOMicah Winkelspecht 说道：“一个连接医药健康产业，将所有医疗平台的重要数据连接到一起的新系统将会因为区块链技术的运用而诞生。区块链技术在数据有效性和安全性方面的优势对于医疗卫生行业来说将会使医院、保险公司和实验室能够实时连接并且即时无缝分享信息，而无须担心信息被泄露或者被篡改。”

Micah Winkelspecht 列举了一个案例：“区块链将会为数据记录和身份管理提供一个公开标准。一个全球化的医疗健康区块链能够将每个病人包含本地医院和医生的记录信息关联匹配一个 ID。基于区块链技术的通用医疗健康 ID 能够减少患者诊疗过程中的医疗错误并保护病人隐私。”

Gem Health 的建立是 Gem 进入医疗健康领域的第一步。目前，Gem 正在建造一个网络基础设施，研发医疗健康领域更多的物联网方案，为未来布局。

BitHealth 是一家研发医疗健康数据存储和保护的区块链技术公司。众所周知，数据隐私、数据可信度以及数据外泄是医疗健康产业中最关键的三个问题。BitHealth 致力于存储并且在全球范围内高效安全地传送医疗健康数据。

如果医疗健康数据在全球范围内传送的过程中因为网络故障而丢失，BitHealth 将会使用比特币区块链技术使其从世界各地任一节点中得到恢复。即便是国际上类似于 BitTorrent 的 P2P 文件分享技术形式，如果出现数据问题，BitHealth 也可以从本地节点恢复数据。

BitHealth 研发的这项技术还可以运用在更多的场景里，包括减少保险费用和其他支出、解决数据复制、医疗记录分散化等问题。保险公司可以用以调取客户的医疗历史记录，医生可以用来调取和记录医疗信息，患者能够用来保护个人隐私数据等。

Philips 是全球范围内医疗健康领域的巨头。2016 年 3 月，Philips 宣布成立 Philips 区块链实验室，这是一个在阿姆斯特丹（Amsterdam）的区块链新兴技术研究和发展中心。Philips 网站上的声明称，他们的区块链项目已经研究了半年之久，并致力于联合 IT 专家、医疗保健专家和区块链开发者

继续对这一项目进行研究。Philips 还表示，他们想要找合作者和开发者共同开展项目，并且在网站上提供了一个表单供用户订阅新闻以及表明他们对此的兴趣。

Philips 的意思是他们非常看好区块链技术在医疗健康领域中的应用。Philips 实验室的创始人 Arno Laeven 也说："一家创新型公司只有持续探索新科技才有可能影响并且为应用领域带来价值。我们的目标是研究区块链技术是否能够开发医疗健康产业中数据交互过程的潜在价值。"

2016 年 6 月初，Philips 对外宣布已经和区块链数据记录初创公司 Tierion 达成合作，共同研究区块链技术在医疗健康领域中的应用。

作为未来世界的基础设施，区块链具有广阔的应用前景，但是不会在短时间内替代现有医疗秩序规则及信息化系统。为了推动区块链电子病历应用早日进入人们的生活，区块链专家、IT 专家以及对区块链应用有浓厚兴趣的人需要通力协作。

8.1.2　保存个人医疗记录

医疗数据是医疗领域非常宝贵的资源，包括病人身份、过往病史以及医疗支付情况等，但这些都是患者的隐私数据。当前，患者的私密信息都存储于医疗部门的中心化数据库或者文件柜里，而信息泄露情况时有发生，比如一家美国医疗保险商曾经泄露 8 000 万病人和雇员记录，另外一家医疗中心曾经泄露 450 万病人的私密数据。

由此看来，由医疗部门管理患者的私密信息已不再是最优选择。随着基因数据检测手段以及指纹数据应用的普及，人们开始担心一旦医疗部门泄露了患者的信息，将会导致灾难性的后果。

通过区块链电子病历实现对患者隐私信息的保密显得迫在眉睫，也是目前人类找到的存储数据的最好方法。

另外，病历数据的质量问题是医疗行业面临的一大问题。错误的数据在很大程度上会导致误诊，而且如果同一份病历同时被多人编辑还有可能造成电子病历无法正常更新，还有可能吸引黑客攻击。因此，现存的医疗数据系统是不

可靠的。

例如，同一个病人有多种不同版本的病历，里面的数据还有很大差异，而接手的医生又没有进行核对的情况下就下了诊断。在这种情况下，病人有可能遭受误诊，引发各种生理、心理、经济损失等问题。

有了区块链电子病历以后，上述问题将不复存在。因为区块链电子病历不在医生、医院以及任何第三方手里进行保存，而同时，所有区块链上的参与者都会共同维护每个人的信息安全。综上所述，区块链可以在一定意义上避免医疗卫生行业误诊或者恶意篡改数据的行为。

可以说，区块链技术是一个集数据库、开放性、安全性等功能为一体的创新技术，可以解决现存医疗数据系统存在的问题。作为有着严密组织架构的授权账簿，区块链能够实时核实和记录所有交易。这种运作模式将会颠覆当前医疗卫生行业的信息处理方式。区块链上的每个参与者都可以保留记录，而所有参与者的信息都是一致的，这就避免了有人恶意篡改系统信息，使区块链上的数据更加安全。

下面我们看一下基于区块链技术的电子病历系统的工作原理。当患者到医院就诊时，医院会将患者的就诊信息上传到区块链上，给患者的病历信息扣上时间戳然后进行加密。这样一来，患者的病例数据就被存储在区块链分布式账本中，不能被随意篡改。另外，患者自己持有区块链电子病历的密钥，任何人都不能随意查看，提高了病例数据的保密性。

建立区块链电子病历系统，在患者允许的情况下，每一个医疗机构都会查看到患者相同的病例信息。

区块链通过一致性算法确保了病历数据被记录的准确性。比如，如果其中一条医疗信息记录患者的血型是 B 型，但是其他医疗机构对相同患者的血型记录是 A 型，那么患者血型为 B 型的信息将不会被记录在区块链中，并且将会在系统中提示信息不匹配。这种方式可以保护患者的医疗病历信息，使患者免去了每次去新的医疗机构就诊时都要重新记录病例数据的麻烦。

区块链电子病历还没有全面推广开来，还有一些问题需要解决。尽管我们还不确定区块链电子病历系统最终会是什么样子，但有一点是非常肯定的，那就是它离不开区块链技术。

8.2
DNA 钱包

区块链技术在数据存储方面的应用将会形成一个 DNA 钱包，使基因和医疗数据只能通过使用私人秘钥来获得。这使医疗健康服务商能够安全地存储、统计和分享患者数据，帮助医药企业高效地研发药物。这种模式的建立对患者与药企来说都是有利的。

8.2.1　利用区块链进行基因存储

当个人基因排序成为一种主流之时，全球 70 多亿的人们需要一个安全的方法来存储基因。个人基因的变化普遍低于 1%，理论上可以被压缩到 4 字节。人类基因大致有 30 亿碱基对，将其存储在比特里是不现实的。

另外，存储基因数据的目的是做染色体研究，而不是在长数据流里无法处理。基于几个变量，个人染色体的数据可以从 50M 变到 300M。简单来说，假设存储一个人的基因数据需要花 600 亿字节（3 亿碱基对 ×2）来存储，可以用 GARLI 技术来压缩这些数据。当时，这些数据被压缩后会在哪里，又如何访问这些技术呢？这些都是基因存储的难点。

成立于 2014 年的 DNA.bits 高科技技术公司主要解决了绘制大量临床数据集的挑战。DNA.Bits 致力于区块链密码学的研究，希望找到一种安全可靠并且匿名的方式来解决数据追踪、标签化、大数据、基因数据分享、健康数据交互引用以及相关的医疗数据问题。DNA.bits 使用比特币平台，能够在不建立中央数据库的基础上聚集不同数据源的数据。

DNA.Bits 认为：“人们对基因、健康以及疾病相互作用的理解与未来的药学、药理学以及预防医学方面的突破密切相关。因为每个人的基因组以及生活方式都不同，这就导致相同的治疗方案在不同的人身上的影响也不同。”

如果 DNA.Bits 成功研制出利用比特币区块链科技来存储基因和医疗病史档案的解决方案，研究人员将可以方便快捷地搜索到基因信息，而且还不侵犯

DNA 钱包的隐私性和个人匿名性。

DNA.Bits 的 CEO Dror Sam Brama 描述了公司的目标："保护病人的隐私，让病人可以搜索、控制其个人医疗记录和基因数据，同时让全人类的基因数据实现人类共享。"

如果 DNA.Bits 的目标达成，医院依然可以使用病例数据，然后据此完善医疗保健制度，同时，制药公司还能够根据这些信息做更有效的药，帮助病人治病。

根据 DNA.Bits 的设想，患者的个人医疗记录和基因数据都会被保存在区块链的侧链上。当需要产生交易的时候，数据就会被移动到比特币区块链上。

在此基础上，DNA.Bits 将通过授权各个平台掌握数据获得售前盈收，也可以收取各个平台交易合约金额所得利润的一部分。而造市者可以凭借将媒体数据持有者、基因数据持有者、卫生组织和消费者连接到一起而获得收入。

对 DNA.Bits 来说，基因持有者、数据的持有者以及任何进行基因相关研究的人都是公司潜在客户，包括基因公司、制药公司、科研所、政府公共卫生部门等。

截至 2017 年，全球制药市场的价值已经达到 10 万亿元。在美国，生物工程产品制药已经达到 20% 以上，而遗传医学市场的价值空间以每年 18% 的速度不断扩大。由此可见，制药行业对患者基因和医疗记录数据的需求是非常大的。

DNA.Bits 做的就是在尊重患者隐私的前提下为这些数据的需求者构建一个系统。利用区块链进行基因存储可以说是最佳的解决方案，但是还需要将这一应用落实。

8.2.2 私人密钥唯一识别

耶路撒冷遗传学和协会中心的 Smadar Horowitz-Cederboim 称："对照检索不断变化的医疗和基因记录并且保护患者的个人身份不被泄露，这在个体化用药以及遗传咨询领域里都将成为行业颠覆者。"

Shaare Zedek 遗传学协会的 Efrat Levy-Lahad 医生称，在以色列，每年死于乳腺癌的女性有 1 000 多名。以色列需要一个保护患者隐私的 DNA 筛选和

分析项目降低乳腺癌患者的死亡率。一旦成功，以色列每年将有 200 多名的乳腺癌患者可免于死亡。

以色列乳腺癌的案例可以推及全球任何一种疾病，但是 DNA 筛选和分析项目当前面临的主要问题是隐私问题。作为一名患者，无论是政府机构、医院、制药公司、保险公司、医疗保健公司，还是任何非营利性机构，都是无法付诸信任的，更不会放心地把隐私交给他们。

区块链技术解决了信任难题，患者不需要相信任何机构和个人，因为保存在区块链上的信息数据是私人密钥唯一识别的。只要患者不允许，没有人知道患者的真实身份信息。上一小节提到的 DNA.Bits 公司就正在致力于这一方面的研究。

可以说，区块链 DNA 钱包的应用对医疗领域的意义重大，将会在一定程度上降低人类的死亡率。我们期待区块链 DNA 钱包应用真正落地的那一天，就算我们等不到，我们的子孙后代也终将因此获利。

8.3 药品防伪

药品防伪不仅是区块链在医疗领域的应用，也是区块链在供应链溯领域的应用场景。与编码防伪技术相似，对于运用区块链技术防伪的药品来说，在药品包装盒表面有一个刮层，底下是一个特别的验证标签，验证标签可以与区块链相互对照来确保药品的合法性。

8.3.1 利用区块链“监视”供应链

药品假冒属于供应链上出现的问题。供应链概念最初是一个具有很大革命性的想法，因为供应链增强了产品转移路径的可见性和控制性。但随着当前产品生产和供应出现极端零碎化、复杂化以及地理分散化的特征，供应链过程的不透明性及缺陷性增加，加大了管理难度。作为一种分布式账本技术，区块链

能增强各行业透明度和安全性的特征有望解决供应链出现的一系列问题。

区块链公开记账的方式使得产品追踪上溯到所用原材料阶段成为可能。在区块链上，记账权不归任何一个人所有，也杜绝了按照个人利益操控数据的可能性。另外，区块链的非对称加密技术可以保证数据的安全性。

目前，正在研究利用区块链技术改善供应链管理的公司非常多，包括IBM、Provenance、BlockVerify、唯链（VeChain）等。

IBM 推出了一项利用区块链追踪高价值商品的服务，客户只需要在安全云环境下就能完成产品真假测试。区块链初创公司 Everledger 正在使用该项服务，试图利用该项服务推动钻石供应链实现透明度，增强非洲市场的规范性。

Provenance 是一家位于伦敦的区块链初创公司，主要研究能够帮助品牌商追踪产品材料、原料和产品起源并向消费者提供实物产品相关信息的网络平台。Provenance 的做法是在供应链系统中部署基于比特币和以太坊的区块链系统，增强供应链的透明度，创立信任感。

Block Verify 也是一家位于伦敦的区块链初创公司，主要研究基于区块链技术的防伪方案，提供包括真伪验证以及帮助专家验证产品真伪在内的服务。区块链的公开透明使得产品无须品牌的信任支撑就能保证正品，而且公司还能够利用区块链技术创造登记他们的产品并监视供应链。

Block Verify 的真伪验证服务可以鉴别出来的产品有调换品、伪造品、被偷产品、虚假交易等。在医药行业中，Block Verify 的区块链技术能够通过供应链追踪确保消费者收到的是正品。

BlockVerify 希望通过研究区块链防伪方案打击产品假冒现象，尤其是药品假冒问题，最终消除因为假冒药品为社会带来的巨大经济损失以及每年几十万人的枉死案例。

唯链（VeChain）是中国首个基于区块链的防伪平台，最先从奢侈品流通溯源入手。区块链创业公司 BitSE 是唯链的母公司。BitSE 成立于 2013 年，最初做的是比特币挖矿芯片、挖矿服务、矿池、区块浏览器等业务，随后又开始研究区块链在股权众筹、游戏、物联网领域的应用。2016 年 1 月，BitSE 推出唯链项目。

2016 年 5 月，唯链发布首款区块链 NFC 防伪芯片和移动端应用。唯链的

防伪方案是在每个产品里放置一个 NFC 芯片，将其唯一 ID 信息写入区块链，从生产、物流、门店、消费者到海关都能共同维护记录信息。通过唯链的应用平台，消费者可以直接查看所购买商品的上游信息，并能写入自己的数据。这种方式还可以加强品牌方与消费者的联系。2016 年 1 月，唯链完成了数百万元的种子轮融资。

在未来，消费者验证药物的真实性就像扫描产品包装盒上的二维码一样简单。因为区块链给每个产品赋予了独一无二的身份，在供应链上的所有权变化都会被记录下来，每个人都很容易进行访问。

8.3.2　轻松识别假冒药品

将区块链用于药品供应链后，我们就可以做到轻松识别假冒药品。由 Linux 基金会领导的超级账本项目就正在进行相关研究，试图通过区块链技术识别假冒药品，以对抗全球泛滥的假冒药品问题。

超级账本项目（HyperledgerProject）的成立时间是 2015 年 12 月，目的是建立一种透明、共享、去中心化的分布式账簿技术。超级账本项目的成员跨越了金融与科技领域，包括 IBM、埃森哲、Intel、思科、JP 摩根、富国银行、芝商所等。

2016 年 4 月 20 日，超级账本项目召开了工作组会议。在会议上，作为超级账本成员的全球专业服务公司埃森哲咨询的代表 Primrose Mbanefo 透露，超级账本项目研究的用于识别假冒药品的区块链项目将会通过不可变更数据来追踪药品，最终不仅会使这个行业变得更加高效，还会增强制药公司的问责能力。

Primrose Mbanefo 是连接设备软件主管，在埃森哲咨询的物联网业务发展团队工作，还协助公司创造了一些概念证明。Primrose Mbanefo 说：“只要我们能够拿到区块链上的数据，证明文件没有被篡改过，我们就可以说所检验的药品确实来自它所声明的地方，而不是假冒的。”

在该工作组会议上，如何精确定义制药行业内的假冒行为成为讨论焦点。Primrose Mbanefo 认为，药品假冒行为不仅包括“流氓”制造商，还包括生产的药品有效成分不达标甚至不含有效成分的知名企业。

在贸易流通顺畅的市场环境里，利用区块链区分假冒药品的想法是非常惹人关注的。在英国，2015 年 6 月开展了一次打击假冒药品的行动，被没收的假冒药品共计 5 160 万欧元。

利用区块链控制药品假冒问题是超级账本项目研究的区块链供应链应用案例之一。在供应链方面，区块链另外的应用场景还有很多，包括追踪产品的生产和组装、评估商品的运输和销售、确认商品标签的真实性等。

2016 年 10 月，超级账本项目新添了 10 名新成员，其中有四个来自于中国。据悉，新加入超级账本项目的公司包括恒生电子、趣链科技、深圳前海招股金融服务有限公司和深圳新国都技术股份有限公司，还有印度国家证券交易所、诺基亚、俄罗斯联邦储蓄银行、Murphy&McGonigle、theLOOPInc 和 PC。

截至 2016 年年底，超级账本项目的成员数达到 95 家。2016 年 9 月 8 日，万达金融集团作为超级账本项目第一个来自中国的核心董事会成员正式加入超级账本项目。

8.4 蛋白质折叠

研究蛋白质折叠的意义在于揭示生命体内的第二套遗传密码。由于蛋白质折叠的速度非常快，过程难以捕捉，斯坦福大学的教授们曾经使用成本高昂的超级计算机来模拟这一过程。这种方式不仅成本高，而且还存在单点故障。区块链技术的运用使他们可以选择借助一个巨大的分布式网络来进行高速运算。很多使用成本高昂的超级计算机的企业都开始关注起区块链在这方面的应用。

8.4.1 排除计算机运算的单点故障

截至 2017 年上半年，还没有公司开始研究区块链在蛋白质折叠方面的项

目应用，相关理论也尚未完善。因此，我们先了解一下当前的蛋白质折叠研究情况。

Folding@home 是一个由斯坦福大学化学系的潘德小组主持的研究蛋白质折叠的分布式计算工程，在 2000 年 10 月 1 日正式启动。Folding@home 是 2007 年吉尼斯世界纪录承认的世界上最大的分布式计算项目。

Folding@home 旨在通过模拟蛋白质折叠过程了解多种疾病的起因和发展，包括疯牛症（牛海绵状脑病）、脑退化症（阿尔兹海默症）、多种癌症和癌症相关综合征等。Folding@home 已经成功模拟 5 ～ 10 微妙的折叠过程，是之前预计的可模拟时段的数百万倍。

截至 2013 年年底，参与项目并且提交成果的人超过一百万，计算能力总和达到了全球超级计算机前十名的水平。

Folding@home 客户端使用了经过修改的 TINKER、GROMACS、AMBER 及 CPMD 四种分子模拟程式进行运算，并且还能不断优化，加快运算速度。

由于 Folding@home 项目的计算原理是高密度分子动力学，所以在 CPU、GPU 等硬件方面的资源消耗非常大。另外，受到计算分子之间长程力的影响，Folding@home 项目计算代码中代码条件分支也非常常见，对 GPU 着色器灵活度有着很高的要求。Folding@home 项目的 GPU 使用量也比较大。

Folding@home 项目对 GPU 最大的考验是流处理器的计算自由度，这就使 GPU 必须拥有更强大的调度能力和缓存体系。

作为一个分布式计算的项目，世界各地的人们下载并运行 Folding@home 客户端，大家组合在一起构成了世界上最大的“超级计算机”。每一台参与的计算机都使该项目距离成功更进一步，让人类距离重大疾病的攻克进程不断推进。

然而，对于 Folding@home 项目来说，构成“超级计算机”的每一台计算机节点也为运算结果的准确性带来了风险。只要发生单点故障，Folding@home 项目就会计算出错误结果，而且没有人知晓。

如此一来，利用区块链技术代替“超级计算机”进行计算可以排除计算机运算的单点故障，值得区块链创业公司进行相关研究。

8.4.2 分布式运算超过计算机

通过上一小节对 Folding@home 项目的讲解，我们知道模拟蛋白质折叠过程需要非常大的算力。但是更多的时候，各种计算机都处于闲置状态，尽管人类对计算资源的需求量增长迅速。那么，我们怎样才能更加合理高效地利用闲置浪费的算力资源呢？区块链技术可以搭建一个分布式网络，解决这一难题。

分布式云计算平台 iEx.ec 联合创始人 Gilles Fedak 说："为了运行大型应用和程序，处理大量数据，各行各业和科学社区需要的算力越来越多"。尤其是产品仿真、深度学习、3D 渲染等领域对算力资源和高性能运算的需求不断增加。

IBM 负责区块链技术的副总裁科莫（Jerry Cuomo）说："压缩时间是超级计算机最大的障碍。而我们对业务流程的完成速度要求越来越高，因此对算力的需求也呈指数级增长"。

物联网分布式账本 IOTA 创始人 David Sonstebo 也认为实现实时计算和克服现有云计算模式延时的问题非常重要，他说："总体来说，计算的最大问题在于生成数据的设备与分析数据的数据中心距离太远"。

SETI@home 计算资源共享平台已经存在很多年了，事实证明通过中央服务商进行任务分配和管理根本无法从根本上解决问题。比如，物联网领域的中心化云计算就不是一个好的解决方案。

在互联网的中心化云计算系统中，边缘云设备会不断生成数据，而数据处理面临着网络拥堵、信号冲突、往返延时、地理距离等挑战。有时候，中心化架构可能会直接拒绝一些软件的产品线，比如分布式应用（DAPP），这就导致雾计算、分布式人工智能、平行流数据处理等无法实现。

David Sonstebo 说："不断发展的物联网对分布式计算有绝对需求，设备只有互相进行实时计算资源交易才能分散计算压力"。

中心化模式的另一个问题是无法实现资源共享。分布式计算平台 Golem 的创始人表示："纵观虚拟化技术近一二十年的发展就可以知道，在数据中心或者个人计算机中搭建任何环境都是比较简单的，但要真正实现出租硬件还是很困难的。由于将不同供应商的设备进行对比是一个复杂过程，找到最契合任

务的解决方案将会花费很多时间和专业性”。

Monax 的 CTO（首席技术官）普雷斯顿 • 拜恩（Preston Byrne）认为，确定参与者已经执行了任务或者保证算力提供者了解了交换价值是支付方面的主要问题。与受信任的机构合作时，这些问题可以很好地得到解决，但如果是硬件和算力参差不齐的节点，那情况就复杂了。

区块链如果能解决以上所有难题，利用区块链技术构建的分布式计算机网络就可以实现共享经济，让所有拥有计算机的人可以出租空闲算力，获得额外收入。另外，区块链和分布式账本的 P2P 特性还能帮助提供算力的设备拉近与数据来源的距离，避免与云设备之间的往返延时。

普雷斯顿 • 拜恩称：“尽管区块链本身不是一个计算平台，但是可以构建出一个连接计算时间的买卖双方的市场应用，使其利用数字货币进行支付，不需要任何中间商”。

IOTA 已经在 Tangle 基础上开发了分布式账本，这个可扩展设计消除了区块，改用有向非循环图（DAG），有助于减少交易时间和费用，是 M2M 环境下分布式算力按需交易模式的核心。

公司社区服务办公室的 Julien Béranger 说：“iEx.ec 采用以太坊区块链搭建了另一个分布式计算平台，这个市场网络平台不仅提供应用和数据，还提供高性能计算。也就是说，任何人都可以通过区块链智能合约提供算力”。

该分布式计算平台利用 Desktop Grid 或 Volunteer Computing 收集世界上闲置的算力，执行大型并行应用。最重要的是，该计算平台的成本远远低于传统超级计算机的费用成本。

区块链使分布式运算的算力大大提高，对此，Gilles Fedak 表示：“在中心化云计算模式下，数据中心通常在偏远地区。而区块链支持去中心化基础设施，可以拉近数据和数据提供者和消费者的距离”。

可以想象，人类未来对算力的需求将会继续增加，而当前的云服务器还不确定是否可以通过升级满足人类对算力资源、成本和速度的需求。值得庆幸的是，区块链给我们带来了传统技术没有实现的可能性。一旦区块链成功运用于分布式运算，更多的项目将会诞生，代替 Folding@home 项目研究蛋白质折叠。

Block chain

第9章
区块链在教育领域的应用

区块链当前主要的应用场景是金融领域，在非金融业，区块链也迅速发展，并受到了重视。这些领域包括上面几章提到的物联网、大数据、医疗等。本章则是大家一起了解区块链在教育领域的探索以及应用。

practice

9.1 教育数据存储与分享

区块链的本质是一个分布式账本，所以区块链在任何领域的应用都与数据存储有关。毫无疑问，区块链在教育领域的第一个应用就是存储与分享教育数据。

9.1.1 区块链储存教育数据

在社会发展中，教育是最基础的工程，是培养年轻力量的根据地。信息时代的到来改变了教育行业，使教育设备、教育系统以及教育环境等纷纷融入了信息化元素，但是也给数据安全带来了威胁。

在教育信息化的大环境下，大部分原来存储于纸上的数据转移到了硬盘和网络上，包括学籍档案、成绩管理、教职员工信息、学术文献资料等。小到院校级别的各种数字教学平台，大至国家级的教育资源和管理公共服务平台，都存储了教育领域的海量知识和用户数据。

教育领域产生的数据是海量的。如果可以有效利用这些数据信息，对于指导教学、实现对教学资源的科学管理有重大意义。而且，越高等级的教育机构所产生的数据信息价值越高，机密性也相应更高。因此，教育领域的数据安全问题是一个重大问题，尤其是主张自由开放的学校网络，经常被黑客锁定为目标。

另外，因为内部监控疏漏或者内部人员故意泄露、合作机构因为拥有一定权限借此侵占信息等导致的信息数据泄露也极大地威胁到了数据存储安全。因此，教育机构应当承担起保护教师、学生信息以及学术资料数据安全的责任，预见并防止数据误用、泄漏或盗窃。

在各个群体中，学生信息是最没有安全保障的。一些倒卖用户数据的人甚

至对外声称，只要是大家听过的学校，包括大学、中学、小学等，学生的数据他们都有。这些人倒卖的大学学生数据包含了学生专业、姓名、学号、性别、年龄、身高、体重、联系方式等，可谓是一应俱全。此外，他们还表示可以拿到“全国中小学生学籍信息管理系统”中的数据，包括学生姓名、学籍号、学校、入学方式、住址、家庭成员等。

一位教育信息化资深人士表示：“学生数据分别存放在各个不同的平台，包括学校、招生办、教育机构等，多样的数据存储渠道使得接触数据人员数量增加，这在很大程度上放大了内部人员泄露信息的风险。”

区块链为教育领域的数据存储安全问题提出了最根本的解决方案。一些教育机构开始寻求区块链的帮助，研发基于区块链技术的教育信息存储系统。

区块链是一个去中心化的分布式账本，它可以将教育信息存储在由全球数以亿计节点构成的网络系统中，保证了信息安全。这种教育数据存储方案不仅成本低，而且无法轻易篡改，安全性极高。

美国旧金山的霍伯顿大学软件工程学院已经开始尝试将区块链用于教育数据存储。在 2015 年 10 月，该学院对外宣布，从 2017 年开始，学院将会以区块链的形式完成有关学业证书的记录，谁都无法造假。

霍伯顿大学的联合创始人 Sylvain Kalache 在一封邮件中写道：“对于企业招聘来说，主管人以后不需要花费大量时间和精力去核实毕业生的教育背景是否属实，因为区块链存储了这些数据而且绝对不是造假的。”

当区块链用于教育数据存储，教育机构在数据存储方面的花费将会大大减少，因为他们不再需要花钱建立自己的数据库。

9.1.2　通过加密可与第三方分享

教育数据存储安全是信息教育领域的首要问题，其次就是数据共享。每个地区的教学素材大多不同，一个学校的不同教师采用的教学方法也都是独特的。如果你去书店溜达一圈，你会发现各地区不同教学内容的书籍，包括人教版、苏教版、冀教版等。即便不考虑学生的选择问题，就连教师在教学过程中向学生推荐的参考资料也都是不同的。另外，不同的老师使用的教学课件也不一样，

这在一定程度上造成了资源浪费。

如何才能通过一个有可靠保障的检索和共享实现教育资源共享呢？区块链便是有效解决教育资源共享问题的技术方案。

教育资源共享的基础是通过区块链对教育资源数据进行分布式存储。教师担任了节点的角色，可以在区块链上发布自己的相关教学应用课件、多媒体课程。与此同时，数据经过多个节点认证后存储于网络上，每条信息有独立的时间戳证明验证，保证了数据所有权属于发布者。

另外，学生资料也可以通过区块链技术实现安全共享，这些资料包括教育经历、工作经历、在线学习工具、课外活动等。对于教育机构来说，数据共享有利于更合理地设计课程、完善学分制度、评估学生群体的资质。

数据共享在出国留学方面也有重要应用。由于国内外信息不对称，在国内很难找到国外教育机构的任何资料，包括学校环境、师资力量、教学水平等。一旦区块链应用于教育领域，构建一个数据安全共享的公共信息平台就不在话下。如此一来，任何人、任何机构、任何时间都可以查询所需要的信息，而且无法对信息进行破坏。

基于区块链技术的DECENT内容分发平台就致力于将以上应用变为现实。作为一个独立开源平台，DECENT 允许任何人在 DECENT 协议之上构建应用。

截至 2017 年年初，DECENT 已经构建完成了可以正常运行的全球网络。接下来的工作就是与区块链对接以及进行顶层建设。DECENT 将大学作为首要突破口，并以此为基础建立整个生态链，形成良好的口碑效应，其他教育机构随之被吸引来。下面是 DECENT 的规划。

初期：邀请知名教育机构、实验室加入，建设基本数据库，目标是保证网络的基础运行，增强其稳定性。这一过程需要 1 ～ 2 家教育机构进行实验，将完善学籍信息管理作为突破口，建设人才信息库。

中期：不断扩大信息收集范围，包括教育机构信息、人才信息、学术论文、实验室等相关信息。这一阶段的目标是形成高等教育联盟体系，建设以高校机构联盟的团体形式来主导，具体公司方式来运营的区块链系统。

后期：将区块链系统由高等教育扩散至中小学教育系统，整合教育资源。

DECENT 的商业模式是通过信息存储、查询、会员制以及教育资源资料

的获取收费。在系统运行初期，网络会产生一定数量的代币，会员需要购买代币来支付查询，存储、下载、查看等费用。另外，任何个人或机构也可以通过发布作品、课件、实验项目以及教育资源等获得代币。在这一系统里，参与者都将会获得相应的收入或者价值。

数据共享对教育领域的变革之大是我们难以想象的，期待这一天的到来。

9.1.3　索尼全球教育借区块链实现数据加密传输

2016 年 2 月，索尼全球教育公司对外宣布一项区块链服务计划。学生可以据此转移自己的数据，比如将大学里的成绩单发送给用人单位的老板。这一服务计划意味着索尼全球教育已经在教育领域基于区块链技术研发出了开放式的安全的学业成绩和进步记录共享技术。

近年来，区块链技术逐渐表现得光芒四射，展现出了巨大的潜力。区块链可以让用户在网络上自由、安全地传输数据，而且不需要第三方中介的参与。在这种方式下，任何人都不可能破坏程序或者篡改数据，除非他能够控制全网 50% 以上的算力。

索尼全球教育公司开发的区块链服务计划实质上是一种数据加密传输技术，利用该技术可以在网络上共享记录，创建一个全新的、安全的基础设施系统，为教育数据存储打开新的大门。例如，你参加了一次考试，取得了非常好的考试成绩，那么你就可以直接将测试结果分享给其他评估机构。

个人评估的方式随着教育范式的发展变化而逐渐多样化，在这种趋势下，不同的评估机构会因为评估方式和评估方法的不同而得到不同的个人测试结果。于是，索尼全球教育研发出基于区块链的数据处理方式。在未来，各个评估机构可以获得相同的个人测试记录，然后对其进行评估。

而且一旦这一基础设施成功建立，其开放、安全的特征将会吸引越来越多的教育机构加入到该系统中。如此一来，各个评估机构对测试结果的评估结果将培养起高信誉度。最后，索尼全球教育建立的基础设施系统将会成为一种开放数据交易协议，从而延伸到教育领域以外更广泛的行业，包括医疗行业、环境服务，甚至是能源领域。

为网络社会建立起全新的教育基础设施，这就是索尼全球教育的使命。索尼全球教育认为，区块链是一种极具潜力的核心技术，在未来，区块链将会塑造出全新的教育景观。

另外，索尼全球教育还发起了一个世界级测试——数学挑战赛。该测试主要考验的是参与者的计算能力以及创造性思维能力。参赛者来自全球 80 多个国家，人数达到 15 万名之多。

在这场比赛里，参与者回答问题的正确与否不是最终得分的唯一决定因素，整体的测试表现也会影响最终得分，包括回答时间、心态等。而最终的得分则体现了参与者能力的高低。

索尼全球教育能否成功研发出基于区块链技术的教育基础设施都将在 2017 年见分晓。到时候，索尼全球教育将会把新的教育基础设施整合到他们自己的服务产品当中，而全球数学挑战赛就是第一个实验。

9.2 区块链教育证书检验系统

在教育领域，很多大学都开设了数字货币课程，比较知名的包括斯坦福大学、普林斯顿大学、麻省理工学院、清华大学等。有些学校还建立了区块链教育证书检验系统，以此确保教育证书的真实性。就像医疗领域用区块链识别假冒药品一样，这是一种新的发展趋势。

9.2.1 伪造文凭已不再有效

对学生来说，在大学里获得的各种证书以及大学档案对于未来就业有着深远影响。但是，由于大学校园里的学生们来自全国各个地区，户口本各不相同，在大学学习期间获得的证书不一样，毕业后又前往不同的公司单位工作，只要任何一个环节出错，都有可能导致信息错误、档案丢失、信息伪造等问题。

有一些区块链创业公司开始利用区块链技术进行学历证书认证，这可以解决伪造文凭的问题。如果更多的学校接受利用区块链技术辨别学历证书、成绩单和文凭认证，伪造文凭等相关欺诈问题将会更容易得到解决，而且还能节约人工检查以及文档工作的时间和成本。

目前，大多数证书管理系统的运行都比较缓慢、复杂，而且不可靠，因此，我们需要为证书创建一个数字基础设施解决这些问题。区块链技术使当前创建一个证书认证基础设施成为可能。这一设施将会帮助用人单位验证员工的学位证书是否是学校颁发的。

2015 年年初，美国麻省理工学院媒体实验室开始研究数字证书，试图为包括学生在内的更广泛的社会群体签发数字证书。证书的本质是一种信号，其含义可能是某人是某机构的成员或者更多。如果你拥有清华大学的学位证书，那么就代表你毕业于清华大学，它将会帮助你找到你想要的工作。

这是一件振奋人心的事情，因为它不仅是最优的证书处理方式，还是可以带领让我们思考未来证书模式的一个机会。区块链提供了一种技术基础，可以让我们存储和管理这些证书。

那么，数字证书的工作原理是什么？数字证书的颁发与验证原理是比较简单的：

首先，创建一个数字文件，这个文件里包含收件人的姓名、发行方的名字、发行日期等基本信息；然后使用一个只有发行人能够访问的私钥，对证书内容进行签名，并为证书本身追加该签名。其次，系统会通过哈希算法验证该证书内容没有被人篡改；最后，发行人使用私钥在比特币区块链上创建一个记录，表明在什么时候为谁颁发了什么证书。数字证书系统可以验证发行人、收件人以及证书本身的内容。

可想而知，当数字证书被研发出来，应用于教育领域，伪造文凭将没有立足之地。

9.2.2　学信网存储数据三大弊端

你或许还不知道，你的学位证、毕业证很有可能被他人“克隆”。克隆学

历甚至可以通过中国高等教育学生信息网的查询。

首先了解一下什么是克隆学历。克隆学历就是找一个跟你同名同姓的毕业生，克隆与其一样的学位证、毕业证。也就是说，不上大学也能拿到大学学历。

按照知情人士的说法，克隆学历分为三个环节。第一步是查询同名同姓的毕业生，从中挑选合适的对象；第二步是通过解码获得包括毕业证编号在内的全部信息；第三步是制作毕业证、学位证和学籍档案。

当前公司人力资源检测求职者学历的真伪只有一个方法，即从学信网查询姓名和证书编号。如果查不到相关信息或者查到的信息与求职者不同，那么说明求职者的学历是假的。如果查询到的证书缺少身份证、照片等信息，实际上也无法确定求职者学历真假。克隆学历就是据此蒙骗过众多公司的。

关于办理伪造高等院校学历、学位证明的刑事案件，最高人民法院和最高人民检察院曾经出台一个司法解释，对于伪造高等院校印章制作学历、学位证明的行为，以伪造单位印章罪处罚；明知是伪造高等院校印章制作的学历、学位证明的行为而贩卖的，以伪造事业单位印章罪共犯论处。

根据《刑法》规定，伪造公司、企业、事业单位、人民团体的印章的，处三年以下有期徒刑、拘役、管制或者剥夺政治权利。

尽管如此，伪造学历、学位证明的行为依然难以杜绝。中国高等教育学生信息网之所以会出现漏洞被不法分子利用，根本原因在于它是一个中心化的信息管理系统，其弊端有三个，内容如图 9-1 所示。

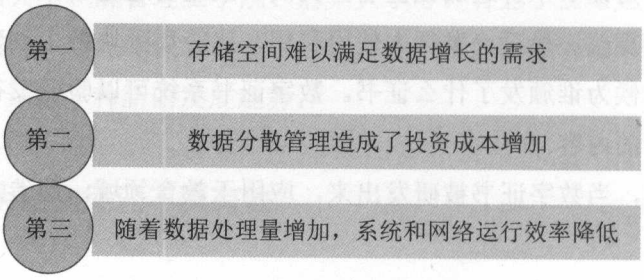


图 9-1　学信网作为中心化信息管理系统的三个弊端

第一个弊端是存储空间难以满足数据增长的需求。高校在校园建设过程中积累了大量的信息数据，这些信息数据存放于各自的独立服务器内置硬盘或直

连存储（DAS）空间里。相互独立的应用系统构成了典型的分散式架构。在校园网络中，服务器上的存储设备通过 SCSI 等总线技术与操作系统紧密整合在一起。单个服务器的每一个 SCSI 通道上最多可以连接 15 个设备，而一台文件服务器对应一台磁盘阵列。

SCSI 的总线结构使直连存储难以大范围扩展。要想增加存储空间容量，就只能不断增加数据服务器的数量。所以说，随着数据的快速增长，中心化的服务器已经难以满足存储空间的需求。

第二个弊端是数据分散管理造成了投资成本增加。中心化的应用服务器和数据服务器越来越多，不仅形成了服务器分散式管理的局面，还直接导致数据中心设备投资成本大幅度增加。对于系统管理员来说，在服务器分散式管理的数据存储方式下，要实现数据库系统的高效管理是非常困难的。尤其是数据恢复以及数据备份工作，管理环节和操作繁杂，非常耗费时间和精力。

第三个弊端是随着数据处理量增加，系统和网络运行效率降低。在网络环境下，数据中心处理业务工作是非常繁忙的，包括数据加载、发布、更新、备份、恢复等操作都需要占用网络带宽和服务器资源。当网络上数据存储量增长到一定规模时，数据服务和数据管理将会造成极大的网络负担，导致系统和网络运行效率较低。有限的服务器和网络性能与不断增加的数据处理量是一对难以调和的矛盾，因此这种模式难以长久运用。

因此，以服务器为中心的网络系统必将向分布式数据网络转变，这是网络存储发展的大趋势。

9.3 学业成绩水平测试

区块链的最初用途是记录和确认每一笔比特币交易，发展到今天，其应用范围已经远远超过了数字货币。现如今，越来越多的行业对区块链技术产生了兴趣，包括教育行业。一些教育机构试图用区块链系统替代学务系统，记录和

验证学业成绩、出勤率等。

9.3.1 比教务管理系统更智能

教务管理系统是教育机构必要的组成部分，其包含的内容对于学校管理决策者有着重要意义。对学生来说，教务管理系统包含着众多有价值的信息，经过快捷查询就能获取对自己有用的信息。

随着学校运营时间的增长，学生数量的持续增长，有关教务的各种信息数据也成倍增长，这对于教务管理系统的运行稳定和效率提供了较高要求。

由于大多数学生都是非常关心自己学业的，所以学校应当开发高效、易于查询并且方便管理员管理的教务信息系统。

采用 SQL server2003 的数据库技术进行架构对教务管理系统构建来说是最简单的方法。这种架构主要包括四个模块，分别为登录、教师用户、管理员用户、学生用户。各个对象可根据自己的权限完成查询。

系统管理员主要负责整理和更新学生以及其他输入对象输入的信息数据。由于信息量非常大，所以管理员需要经常对教务管理系统进行维护和更新，防止系统出现运行、信息失误等问题。

比起传统人工传递工作，采用教务管理信息系统可以减少很大一部分人工开支，降低信息管理成本，而且增加了获取的信息量、缩短了信息处理周期。教务管理信息系统有利于教育机构规划教学资源、提高学生信息以及反馈教学信息的利用率。

尽管教务管理系统对教育机构的作用很大，但是区块链的出现依然完胜教务管理系统。因为区块链成绩单比教务管理系统更加智能，应用范围更广。作为公开可见的分布式账本，区块链记录的信息数据可以永久存储且无伪造的可能性。

区块链成绩单是这样的：这里保存着每一个学习者的基本信息、学习过程、考试成绩、课程设置等数据，没有人可以篡改。每个学习者可以根据自己的时间安排选择必要的课程学习，参加重要的考试，相对来说比较自由。对于用人单位来说，这些记录都是公开可见的。

长期以来，学习者的学习成绩等档案都是由学校保存管理的，但是区块链成绩单将会改变这种传统。自此之后，学习者将可以自主管理其学习过程和结果的记录及证据。而且利用区块链技术呈现学习者学习的过程和结果将成为主流。区块链成绩单可以记录的数据包括学习者全部的成长经历、学习过程和结果、完成的学习项目、掌握的技能、他人的评价等。

与教务管理系统相比，区块链成绩单对学习者的帮助会更大。随着学习环境向技术赋能的方向发展，课程选择以及学习成果认证对学习者来说意义重大。区块链成绩单将会提供这样一个机会：学习者可以从众多教学机构中自由选择想要学习的课程，然后得到学习成果认证，并将自己的学习成果、兴趣爱好和技能特长等展示给用人单位。

此外，有了区块链成绩单，学习者在转学的时候不再需要向相关学校申请开具学习证明、成绩单等转学手续。因为通过区块链成绩单就可以了解学习者的学习内容、过程和结果，包括学习的课程性质和内容、完成的作业、独立以及团队完成的项目、考试类型及成绩等。

新的信任网络也将会基于区块链成绩单形成。学习者可以在网络中识别其他学习者掌握的知识和技能，据此建立起基于学习过程和结果的社交网络系统。

区块链成绩单有利于学习者创建、维护和共享个人学习资料，包括所学课程、学分、成绩和经历等。在此基础之上，学习者的学习过程和成效将会得到明显改善。

如果区块链成绩单能够应用并普及，教育机构的运营成本将大大降低，学生的文凭成本也将跟着下降。另外，区块链教育系统还能够防欺诈，降低教育领域违法案件发生的可能性。

教育数据存储与分享、教育证书检验、区块链成绩单是区块链在教育领域最主要的三大应用。除此之外，区块链还可用于学习账本、教育区块链等。“学习账本”与“教育区块链”是美国两个非常著名的智库机构“未来研究院”（Institute for the Future）和 ACT 基金会（ACT Foundation）联合提出的，其核心思想是“学习即收入”。

具体来说，一个教育区块链表示学习者完成一小时的学习成效，教育区块链可以被学习者赠送给他人，而学习账本的作用是追踪教育区块链中存储的知

识和技能。无论是在教育机构，还是在工作场所，学习者都可以通过学习获得教育区块链。而学习账本则可以帮助学习者无论是在什么场所都可以赚取学分和认证。另外，学习账本还可以体现学习者的个人兴趣爱好或业余活动。根据学习者的教育区块链，企业可以招聘到需要的员工。

更厉害的是，学习账本和教育区块链的提出者认为，学习者的实时收入有望被追踪，从而发现可以给学习者带来更高收入的知识、技能、课程或专业，为其他学习者提供参考意义。如果这一切成为现实，学习者还可以利用学习账本寻找投资人。因为学习账本可以追踪、记录教育区块链为学习者带来的收入，如果投资人认为收入非常可观，便可以向学习者投资，要求获得学习者收入的一定比例作为其投资回报。两者之间的投资协议将会以智能合同的形式存在。

学习账本的构建离不开区块链，这也意味着区块链的特征会体现在学习账本上，即学习者获取的所有教育区块链都将记录在学习账本上，永远保存而且无法轻易篡改。

学习账本与教育区块链生动地描绘了人类学习和职业发展的未来蓝图，也反映了区块链在教育领域中的应用具有无限价值和潜力。

9.3.2 全球第一所接入区块链技术的学校

美国旧金山的霍伯顿大学是全球第一所接入区块链技术的学校。在 2015 年 10 月，霍伯顿大学软件工程学院对外宣布，从 2017 年开始，学院将会以区块链的形式完成有关学业证书的记录，谁都无法造假。

塞浦路斯是最大的私立大学尼科西亚大学，也是最早使用区块链技术的大学之一，该学校将学生的获奖情况放在区块链上保存。尼科西亚大学的教师 George Papageorgiou 称：“区块链的使用获得了很好的反响，学生会表示非常愿意使用这项新技术。”值得注意的是，尼科西亚大学也是第一所提供数字货币课程的大学。

区块链技术进入教育领域以后，基于区块链技术的比特币也开始在学校流行起来。一些大学已经在校园里装上了比特币取款机，校内商店也逐渐接受比特币这样的支付方式。其实，让学生们尽早接触数字货币以及区块链技术是必

要的，毕竟随着数字货币以及区块链的应用范围扩张，很多学生在毕业后都需要接触到这一领域。

总之，区块链技术在教育领域的应用有利于简化教育系统、防止学历伪造，为学生、学校和用人单位提供了证书获取、认证和分享的一站式平台。

除了之前提到的霍伯顿大学软件工程学院以及本文所说的尼科西亚大学，全球众多教育机构和科技企业已经开始投入资源探索区块链技术在教育领域中的应用。针对区块链技术在教育中的应用前景，区块链研究者 Watters 认为存在五大挑战，内容如图 9-2 所示。

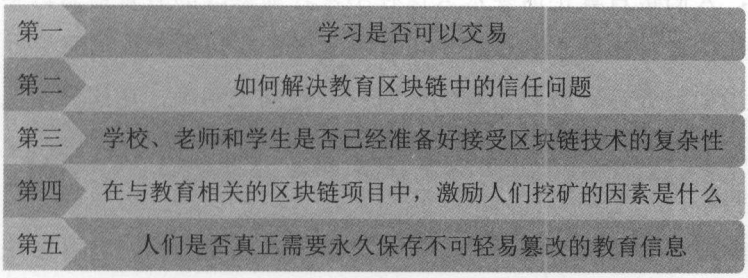


图 9-2　区块链技术在教育中的应用前景五大挑战

第一，学习是否可以交易。作为分布式账本，即便是在金融领域之外，区块链的用途依然是记录各种交易。那么，在教育领域，这些交易都是什么呢？它们是完成课程、考试、发表论文、出版图书，还是对所学习内容的点赞或收藏？此外，在记录上述交易活动时，学习者得到或失去的具体指什么？这些都是需要研究思考的问题。

第二，如何解决教育区块链中的信任问题。区块链技术的广泛应用打击了银行、清算公司等以信任为基础的传统机构，因为去中心化的区块链技术将挑战甚至取代那些中心化机构，随之而来的是全社会信任机制的变化和混乱。

在教育区块链中，学生被视为不可信对象，他们所掌握的知识、技能、证书或文凭等只有经过认证才具有可信度。但是，区块链技术如何验证颁发资格证书的机构？如果按照交易量的话，相当于变相鼓励这些机构滥发证书，这成为区块链研究者需要解决的一个难题。

第三，学校、老师和学生是否已经准备好接受区块链技术的复杂性。区块

链技术的应用基础是应用公共密钥，并拥有庞大的运行区块链节点的计算能力，但是教育机构做好准备了吗？分布式、去中心化的技术并不是提升教学绩效的最佳方案，那么应用区块链技术提升教学绩效的可能性有多大、如何实施具体方案？

第四，挖矿是区块链创造新区块的过程，这一过程通过花费大量的计算资源获得比特币。那么，在与教育相关的区块链项目中，激励人们挖矿的因素是什么？此外，与教育相关的区块链项目是继续利用比特币挖矿模式还是构建像以太坊一样的第三方平台？

第五，人们是否真正需要永久保存不可轻易篡改的教育信息。学习是一个人成长变化的过程，而永久保存不可轻易篡改的学习者个人信息有什么意义和价值，应当如何处理？教育数据的所有权问题尚未明确，在这种情况下，学习者如何管理并控制区块链中的个人隐私？学校有权将区块链中的学生数据卖给其他机构吗？

如果学习者希望将一些不光彩的过去抹去，重新开始，教育区块链如何解决这一问题？一旦区块链技术的应用使得学习者的数据公开引发另外一些问题时，谁充当监管者，谁负责？

因此，即便教育领域对区块链技术持有乐观态度，相关研究者依然要谨慎思考上述问题。尽管区块链技术在教育领域中的应用面临众多挑战，但是毋庸置疑的是，从学校、教育行政管理机构到从事教育培训的商业企业，都已经意识到区块链对教育领域的巨大变革潜力，因此纷纷投入资金、技术等资源，从事区块链在教育领域的应用研发。

总之，我们应当抱着开放、包容的心态，积极迎接区块链技术可能给教育领域带来的改变，为推动区块链应用落地做好心理、知识和技能上的准备。

Block chain

第10章
区块链在公证领域的应用

公证是一种公证机构对事实和文书的真实性、合法性予以证明的活动。传统的公证过程具有手续烦琐、处理低效等不足。而区块链在公证领域的应用将有助于维护一个安全存放、基于时间戳记录的区块链账本，并将提高数据证明过程的透明度，在明确权属的同时节省成本、提高效率。

practice

10.1 身份认证

当前的身份认证依赖于身份证、户口本等各种证件。然而，很多人都有粗心大意不小心丢失了重要证件的时候，这时候已经不是补办麻不麻烦的问题，而是给自身生活带来不便，甚至影响人生大事的问题。

10.1.1 “你是你”很难证明吗

在日常生活中，很多人都遇到过各种奇葩证明，包括“你是你”“你是单身”等。这些事情听起来可以一笑了之，但如果让我们自己遇上，就是一个非常让人头疼的事情。

一位西南大学的在读硕士研究生就因为不能证明“自己是自己”而错失了公务员体检的机会，尽管他的笔试、面试成绩都拿到了第一。事情是这样的，该硕士研究生是西南大学法学院应届硕士毕业生，他报考了中山市教育和体育局纪检监察岗岗位。尽管他拿到了笔试面试均第一的成绩，但是却在体检前两日丢失了身份证。

为了证明“自己是自己”，他出示了户口本原件、户籍所在地公安部门开具的户籍证明、护照以及机场公安部门开具的临时身份证明等。不幸的是，他依然因为不能有效证明自己的身份而错失了体检资格。

事发之后，中山市人社局针对此事公开作出回复称：“根据《广东省2015年考试录用公务员公告》相关规定，居民身份证是考生参加考试或体检的唯一居民身份证明，临时居民身份证是唯一可代替身份证的法定居民身份证明凭证，因此该考生不得参加此次体检。”

中山市人社局还解释说：“根据《广东省 2015 年考试录用公务员公告》的附件 3《广东省 2015 年考试录用公务员报考指南》第 28、29 和 30 条规定，已对遗失身份证如何参加考试或体检，或其他证件能否代替居民身份证参加考试或体检作出明确说明。作为以上规定的执行部门，为确保公务员考试的公平公正，必须严格依法依规办事，因此我局及时告知其不得参加此次体检。”

根据规定可知，该硕士研究生丢失了身份证的唯一解决办法就是办理临时身份证。然而，由于他是在公务员体检前两天丢失的身份证，而临时身份证办理至少要三个工作日，所以根本无法赶上体检时间。

对此遭遇，该硕士研究生非常愤怒，并在微信朋友圈发出了自己的质疑：“体检前出具身份证的目的是证明身份，户籍作为身份证的母本为什么不能证明身份？况且我还有其他一系列资料，足够组成证据链证明身份。虽然说工作人员是按照规定办事，但是‘仅有身份证及临时身份证作为身份认定依据’的规定，是个正常人都会觉得不合理。”

那么，居民户口本、护照、工作证、驾驶执照、学生证等证件能否代替居民身份证参加考试或体检呢？

《广东省 2015 年考试录用公务员报考指南》第 29 条对此作出规定：“居民户口本、护照、工作证、驾驶执照、学生证等证件都不能代替居民身份证参加考试或体检。居民户口本虽载有个人相关文字信息，但只能证明是家庭成员之一，因没有照片而难以辨别是否与持簿人相符；护照、工作证、驾驶执照等证件虽同样载有个人信息及照片，但反映主题各异，发证机构出自不同部门，主管部门分属各个领域，辨别证件真伪标准不一、难度大；只有居民身份证是由公安部门统一归口管理，是证明居民身份的法定证件。”

在当前的环境下，该硕士研究生的遭遇是难以避免的。但是在未来，当区块链技术应用于身份认证之后，上述尴尬情况可以得到解决。

本书在 3.2.1 小节中讲过，区块链技术可以用于用户的身份验证。由于用户掌握的私钥是唯一的，所以身份验证显得非常容易。下面一起看中本聪通过比特币的创世块证明自己身份的原理。

比特币的创世块有 50 个比特币，而且代码是确定的、唯一的，这就使这 50 个比特币不能使用。中本聪的创世块地址为“1A1zP1eP5QGefi2DMPTfTL

5SLmv7DivfNa”，很多比特币爱好者还向中本聪的地址捐币，使其余额超过了 50BTC。对中本聪来说，他拥有这笔比特币的所有权，但是没有使用权。

比如说，一个比特币的狂热爱好者在网上发言，并妄称自己就是中本聪本人。如果中本聪自己觉得有必要澄清，就可以使用创世块的私钥签名，并注明该发言并非自己本人发出，全世界的人们就知道真相了。

对于所有需要证明身份的场景来说，区块链可以替代身份证的作用。首先，我们需要使用比特币 QT 钱包（比特币本地钱包）生成一个收款地址，该收款地址可以是空地址，不需要有任何余额。其次，我们需要用 QT 钱包对生成的空地址进行签名。签名一般都是使用特定消息，然后就可以得到签名结果。然后，我们需要向全世界公布自己的比特币地址，包括特定消息和签名结果。这时，全世界都知道了这个地址是我们的。

如果是参加考试或体检，考生需要证明自己的身份，那么对方给出一个特定消息，考生只需要签名，对方进行验证即可证明身份。用区块链验证身份的唯一风险就是私钥被盗，显然，私钥被盗的可能性远远小于身份证跟钱包一起被盗的可能性。

区块链让人类第一次不需要依靠任何第三方中心机构就可以完成身份验证，也是人类第一次在互联网上创造了一个不能复制、不可伪造的数据库。等到区块链技术发展到一定阶段，身份证明、出生证明、结婚证明都有可能记录在区块链上。

10.1.2 区块链造就“世界公民”

出国旅行，护照是最重要的证件。很多人出国没有意识到护照的重要性，随意涂改护照内容或者粗心将护照弄丢，给自己制造了很大的麻烦。

小程就因为涂改护照内容而使得德国旅行计划泡汤。事情是这样的，拿到护照后，小程发现护照上自己的出生年月中的月是英文打印的，于是便用签字笔将其划掉，并用红笔在下面附上相应数字。同时，他还用红笔将护照内几枚模糊印记的中国验讫章的年月日描绘了一遍，以为这样可以方便德国出入境官员辨识。结果可想而知，小程被德国法兰克福机场以涂改出入境证件为由拒绝

入境，原机遣送回北京机场。

上海籍旅客小刘和妻子以及一双小儿女也因为护照问题使韩国旅游计划泡汤。原来，小刘和妻子带着两个孩子一大早就出发去韩国旅游，然而两人在飞机上被两个孩子弄得焦头烂额之际竟马虎得将四人的护照当作垃圾一起扔掉了。等到四个人到了韩国金浦国际机场后发现护照不见了，又因为语言沟通不畅没能找回护照。于是，四人被原机遣返。

护照问题有没有更好的解决方案呢？区块链可能为护照提供一个更好的解决方案。“世界公民护照”的创新就是基于区块链技术的护照问题的解决方案。“世界公民护照”是由一个名为克里斯托·弗埃利斯（Christopher Ellis）的比特币狂热信徒开发的一款软件，还曾经被美国《连线》杂志报道。该软件利用的是 PGP 加密软件和比特币区块链，可以创造出以精密数学为基础的身份证明文件，这种证明文件是无法被伪造的。

2015 年 3 月，管理学专业的学生詹妮娜（Janina）成为世界上第一个参与该创新的人，被人们称为“第一个持有加密护照的世界公民”。作为第一个“吃螃蟹”的人，詹妮娜称自己是非常幸运的，并在当天录制了过程视频。自此，詹妮娜成为加密护照的“封面女郎”，同时也成为以区块链技术为基础建立经济共和的坚定倡导者。

克里斯托·弗埃利斯表示：“我们之所以选择詹妮娜，是因为我们希望‘第一个加密护照持有人’由一个不参与开发的人员来完成。这项设计如果能够推广开来，将为人们提供一个简便、有效的方式证明自己的身份，这种讨论超出国界的限制。该‘护照’可以适用于互联网核查之类的功能，未来还有可能为政府提供一个很好的解决方式以省去目前政府集中管理的护照问题。”

区块链造就世界公民的原理是什么呢？首先，我们需要使用比特币 QT 钱包（比特币本地钱包）生成一个收款地址，该收款地址可以是空地址，不需要有任何余额。其次，我们需要用 QT 钱包对生成的空地址进行签名。签名一般都是使用特定消息，然后就可以得到签名结果。然后，我们需要向全世界公布自己的比特币地址，包括特定消息和签名结果。这时，全世界都知道了这个地址是我们的。

此后，如果我们要出国旅游就无须办理护照，要向对方证明我们的身份，

那么对方给出一个特定消息，我们只需要签名，对方进行验证即可证明我们的身份。

用区块链验证身份的唯一风险就是私钥被盗，所以只要用户妥善保管好自己的私钥，别人就无法伪造用户身份。

区块链让人类第一次不需要依靠任何证件就可以完成身份验证，也是人类第一次在互联网上创造了一个不能复制、不可伪造的数据库。如果我们都成为世界公民，以下场景将会成为事实。一个英国海关官员对某个中国游客说，“先生，请对这一消息‘welcome to England’，在您的比特币地址‘×××’上签名。”该先生拿出手机，点了点，官员也在他的桌面设备上点了点，然后说，“welcome to England，×××”。

区块链作为一种颠覆性技术，造就世界公民的意义在于有利于促进全球化的“经济共和”。在人类历史上，全球经济上的共和至今还没有到来，而区块链技术为人类历史上第一次实现经济共和提供了可能性。

这种可能性体现在四个方面：第一，区块链透明、不可篡改等各种特性是实现经济共和的基础；第二，区块链通过 P2P 价值网络使参与经济活动的个体完全对等；第三，区块链的共识机制可以充当经济共和中的“宪法”；第四，区块链中没有中心化高权节点，所有节点共同维护体系稳定。

“经济共和”会如何改变我们的生活呢？经济共和意味着在世界范围内，所有人拥有的经济权利平等。在以区块链技术为基础的经济运行方式里，个体的权利由预先设定好的共识机制或者经过签署的智能合约决定，这将使经济全球化实现最大化地自动运行。这种经济共和具有以下三个特征，内容如图 10-1 所示。

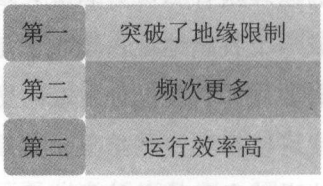


图 10-1　经济共和的三个特征

第一，区块链技术驱动的经济共和突破了地缘限制。区块链达成的共识机

制可以使人们轻易地与其他国家的任何一个人一样平等地拥有经济权利。

第二，一个人的一生可以不参与任何政治活动，但是却离不开经济活动。与政治活动相比，经济活动的频次要频繁得多。

第三，基于区块链技术的经济活动可以通过自动执行智能合约提升当前经济的运行效率，同时根据用户意愿进行财物交易等经济活动。

区块链或将以一种全新的方式创造人类经济活动的高峰，一个全球化的无阻流动的经济已经在我们眼前展现：你可以随时加入或退出区块链系统，只要网络正常运行，就能在 10 分钟内完成任意位置任意资金量的转移。此外，区块链系统实现的资源配置远远超过了货币的范畴。

比如，美国和欧洲曾经封锁伊朗石油，导致伊朗的石油无法走出国门，极大地影响了伊朗的经济。如果运用区块链技术，问题就很好办。伊朗可以直接利用石油燃烧发电，然后将大量的电用来挖矿，获取数字货币。仅仅是一个简单的网络通信，伊朗就可以将庞大的石油资源转化成数字货币，然后在 10 分钟内到任何一个交易所进行兑现，换成外汇。如此一来，美国和欧洲的经济封锁就可以打破。

10.1.3　微软发力区块链的身份认证系统

2016 年 8 月，微软宣布和区块链巨头 ConsenSys、区块链初创公司 Blockstack Labs 以及其他区块链研发者合作开发基于区块链的身份识别系统。微软表示，该研发计划致力于打造出一个开源、高度自治、基于区块链技术的身份识别系统，该系统将会跨越区块链、云服务商和组织，让产品、用户、应用和服务进行交互。

微软在官方博文中写道：“通过这次开源合作，我们计划打造一个跨链的身份识别解决方案，这一解决方案可以扩展到未来任何区块链或者新型分布式系统上。”另外，微软还在 Azure 区块链平台上线了一个开源框架，开发人员可以基于这个开源框架设置“身份识别层”，并且测试其对应用开发的作用。

在区块链领域，研发区块链身份认证应用的公司不只是微软一家。2016 年 8 月，美国国土安全部（DHS）科技理事会资助了四家研发身份认证的

区块链创业公司，包括 Digital Bazaar、Respect Network、Narf Industries 和 Celerity。这是一个小企业创新研究计划（初始 SBIR），这四家公司分别可以拿到 10 万美元的资助。除此之外，美国国土安全部还要求这四家公司研发区块链技术在隐私保护方面的应用。

区块链技术将会颠覆现有的身份认证系统，并创造新的玩法和方式，这是必然的。在这场变革中，Digital Bazaar 主要研发用于发布身份证明信息的关联数据账簿架构。而 Respect Network 主要研发基于公链的中心化注册和发现的服务。

Narf Industries 主要研发的是基于私链的身份认证管理系统。该系统具有真实性、保密性（有选择性地公开信息）、实用性、伪匿名性等特点，而且只允许美国国土安全部进入。Celerity 主要研发基于区块链的身份信息交易平台，用户可以在该平台上与公共和私人组织交换身份信息，而且不需担心信息安全问题。

事实上，这四家区块链创业公司不仅能够拿到美国国土安全部的 10 万美元，还可以拿到更多投资。而是否有机会获得投资人青睐，取决于他们未来研发出的项目成果以及商业模式的潜力大小。

美国国土安全部的小企业创新研究计划是从 2015 年 12 月开始的。身份认证管理是他们投资区块链领域的第一个方向。区块链专家克里斯多夫·弗兰科（Christopher Franko）说：“无论美国国土安全部选择投资区块链技术的哪一方面应用，都将备受瞩目。现在，他们首先选择了身份认证管理，这也很正常。我非常好奇他们将会如何使用这种区块链身份认证系统，毕竟他们投资的四家公司我之前从未听说过。”

克里斯多夫·弗兰科还说，如果可以知道美国国土安全部的投资标准就好了，这样就可以帮助更多有意义的区块链解决方案被发掘。

全球四大会计师事务所之一安永也开始涉足区块链身份认证管理领域。2017 年 3 月初，安永内部人员透露他们正在为一个澳大利亚客户研发新项目，这个新项目就是基于区块链的身份认证管理平台。

安永表示，这一平台将会用于管理和验证客户身份信息，而且还能解决内部数据管理和隐私两大问题。截至 2017 年 3 月 2 日，安永已经在以太坊将该

平台整合完毕。区块链初创公司 BlochExchange 就是安永的这位澳大利亚客户，他们主要研发基于区块链技术的抵押贷款平台。

安永金融服务实践部的经理迈克尔·马罗尼（Michael Maloney）表示："这个区块链身份认证管理平台是我们内部研发团队推出的最切实可行的产品，也是目前我们对以太坊最稳定有效的研究，极大地凸显了以太坊网络的优势。"该项目的研发也表明，安永对区块链重塑金融服务领域的信心是非常强大的。

安永研发的区块链身份认证管理平台能够通过执行传统 KYC 政策（充分了解你的客户）的流程创建客户的身份信息，然后将这些信息分配给区块链中其他受信任的成员。

BlochExchange 的 CEO 安德鲁·科平（Andrew Coppin）对于这一身份认证管理平台的表现非常惊讶，尤其是在第三方数据存储和验证方面的能力是他远远没有想到的。他还说："这一平台给我们带来的优势在于我们在市场上掌握了一种拥有公信力的稳健系统。在此基础上，我们还能与其他有潜力的公司合作，并使他们也获得基于这一平台的优势。"

总体来说，安永将区块链视为一种基础技术，并坚信它可以在特定平台上发挥优势。安永区块链和分布式架构战略主管安格斯·钱皮恩（Angus Champion de Crespigny）也说："身份信息对每个人来说都是非常重要的，我们认为这是区块链应用领域的重点之一。"截至 2017 年 3 月 2 日，区块链身份认证管理平台项目已经在展示阶段，也经过了验证和测试，不过安永具体部署这一平台的时间尚在协商中。

对于区块链身份认证管理技术，安永是非常有信心的，并认为从技术角度来说，区块链身份认证管理平台的应用以及发展不会有什么大的阻碍。安格斯·钱皮恩还说："区块链身份认证管理平台解决了三大核心问题，即 KYC、客户管理和监管问题。从长期发展目标来看，安永还计划研发一种基于这一平台的'担保产品'，用于降低使用区块链技术的风险。"

安永合伙人詹姆斯·罗伯茨（James Roberts）补充说道："我们正在和三家澳大利亚的大型银行保持联系，讨论这一平台的部署问题，不过目前相关的讨论仍然处于早期阶段。"

研发区块链身份认证系统的公司还有很多，包括 IBM、德勤等。可以说，

区块链身份认证系统的应用落地可期。

10.2 产权认证

如果你对房产买卖有一些了解的话，你应当知道，买房是一件非常麻烦的事情。无论是新房还是旧房，都需要办理各种手续和证明。可以说，买房是一件耗费人力物力和时间成本的事情。如果是买二手房，还需要担心是否存在产权纠纷。总之，买房需要耗费一些精力。想象一下，如果房屋产权保存在区块链里，那么购房将变得非常简单，而且还能降低人力成本和发生错误的概率。

10.2.1 复杂的传统资产确认程序

只要是买房，就需要办理房产证，无论是买期房、现房还是二手房。在当前的产权保护制度下，办理房产证是确保房屋产权必须办理的手续。很多人买到房子后，不知道怎么办理房产证。下面一起来看看房产证办理流程。

第一步：确保开发商已经办理初始登记。如果开发商不办理初始登记，购房者是无法办理房产证的。通常来说，开发商主管部门办理初始登记需要20～60天。所以，在购房后的2～3个月之后，购房者可以向开发商询问初始登记是否已经办理并在《购房合同》中对其加以约定。房屋初始登记的情况在本地的房地产交易信息网站也可以查到。

第二步：到房屋所在地的房屋土地管理局领取并填写《房屋所有权登记申请表》。填写好《房屋所有权登记申请表》之后，需要拿给开发商由其签字盖章。有的开发商为了方便购房者，手里有现成的盖好章的表格。如果是这样，购房者只要到开发商处领取《房屋所有权登记申请表》然后填写就行了。办理房产证之前，购房者应当先询问开发商，确定自己办理房产证首先应当去哪个部门，然后直接向该部门咨询，这样就可以免去奔波之苦。

第三步：拿到测绘图（表）。测绘图（表）是办理房产证的必备材料，因为登记部门是根据测绘图(表)确定房产证上标注面积的。购房者拿到测绘图(表)的方式有三种：一是携带身份证到开发商处领取；二是到开发商指定的房屋面积计量站领取；三是向登记部门申请对房屋面积进行测绘，拿到测绘图（表）。

第四步：领取相关文件。办理房产证需要携带的申请文件包括购房合同、房屋结算单、大房产证复印件、开发商审核并盖章的《房屋所有权登记申请表》等。

第五步：缴纳产权登记费、公共维修基金、契税等费用。产权登记费用如表 10-1 所示。

表 10-1　产权登记费

房产类型	价　格	其他费用
居民住宅	每套 80 元	如有共有权证增收工本费 10 元 / 本
其他房产建筑	面积 500（含 500）平方米以下的每宗 200 元，500 ～ 1 000 平方米的为 300 元，1 000 ～ 2 000 平方米的为 500 元，2 000 ～ 5 000 平方米的为 800 元，5 000 平方米以上的为 1 000 元	如共有权证增收工本费 10 元 / 本

根据 2017 新房产契税政策，契税税率如表 10-2 所示。

表 10-2　契税税率

房产类型	税　率
普通住宅	对个人购买家庭唯一住房（家庭成员范围包括购房人、配偶以及未成年子女，下同），面积为 90 平方米及以下的，减按 1% 的税率征收契税，面积为 90 平方米以上的，减按 1.5% 的税率征收契税；对个人购买家庭第二套改善性住房，面积为 90 平方米及以下的，减按 1% 的税率征收契税，面积为 90 平方米以上的，减按 2% 的税率征收契税；对个人购买家庭第三套房或以上套数，不论房屋面积大小，契税税率为 3%，没有减免情况
非普通住宅（高档住宅如别墅等）	3%

关于公共维修基金，每个城市的收取方不同，有的是房产所在地区的小区办，有的是开发商代收，还有的则是银行代收。不管是谁收取，购房者都要保存好缴纳凭证。还需要注意的是，维修基金的具体标准是由当地房产行政部门确定的，各个地区因为经济水平不同会有所差异，购房者应当到当地政府网站或房管局网站进行查询。

此外，嘱咐大家在上交产权登记费、契税、工本费时，需仔细核对房产证的记载，包括权利人姓名、权属状态、面积、位置等重要信息。

第六步：提交申请材料。申请材料准备齐全后，购房者需要将申请材料上交给管理部门。上交的申请材料主要包括开发商审核并盖章的《房屋所有权登记申请表》、购房合同、签订预售合同的买卖双方关于房号、房屋实测面积和房价结算的确认书、测绘表、房屋登记表、分户平面图两份、专项维修资金专用收据、契税完税或减免税凭证、购房者身份证明（复印件核对原件）、房屋共有的提交共有协议、银行的提前还贷证明。

第七步：在规定时间内领取房产证。在提交房产证办理申请后，管理部门会给购房者一个领取证书的通知书，购房者要将通知书保管好并按通知时间及时领取房产证。

在这里，提醒购房者们，交房后千万不要忘记办理房产证，毕竟房产证是房屋所有权归属的重要证明。

有时候，办理房产证会遇到程序上的麻烦，这是一件真正让人烦心的事情。但是，对于购买二手房的人来说，房产证的真假辨别是一件更为棘手的事情。

一个房子少说几十万，多则几百万，如果遇上持有假房产证的假业主，不仅得不到房子，还赔上了一生积蓄，惹上官司，这是购买二手房的人最担心的事情。

一家地产公司分店店长表示，他从业五年多，只有一次在房地产交易登记中心现场遇到假业主卖房。他观察发现，假房产证一点都不正规，稍微有点经验的人都能看出来。

对于购房者来说，见到房产证的机会不多，那么如何识别房产证真假呢？下面介绍八种方法。

第一，看印制房产证的纸张是不是印钞纸。印钞纸是假证永远都不能突破的瓶颈，只要确定房产证的纸张不是印钞纸，就可以确定其为假证。假证使用的印制纸张一般为普通纸张，比较粗糙，通过观察纸张的质量、色泽一般可以辨别房产证的真伪。

第二，电话或者网上查询。产品证号对于房产证就像身份证号对我们每个人一样，是一一对应的。通过各地房产管理局网站或者给出的电话查询产权人姓名、产权证号等也可以辨别真假证。目前，只有部分地区提供房屋产权信息查询。

第三，房产局查询。如果要查询详细的房产证信息，包括：房屋所有人名称、产权证号、登记核准日期、建筑面积、房屋设计用途、权利来源、房屋是否抵押、是否被查封等，就需要携带个人身份证件及房产证到当地的房屋管理局档案馆或者窗口查询。

第四，对比查询。是真是假，一经对比就很容易确定。如果不确定房产证真假，可以找一本同年代、同版本的房产证进行对比。没有任何一本假房产证可以做到与真房产证不差分毫，包括字体、字号、印章等各个细节。当然，对比查询的前提是能够找到同年代、同版本的真房产证。

第五，与人民币的水印设计类似，真房产证也有这一设计，对光观察可以看到宋体“房屋所有权证”底纹暗印，透过光线可见高层或多层水印房屋。显然，假房产证做不到这一点。

第六，全国各个负责发放房产证的市、县发证机关的建房注册号都是不一样的。在判断房产证真假过程中，不仅要看房产证上是否有编号，还要核对一下该编号是不是建设部公告的全国统一编号。如果不是，则房产证一定为假。

第七，真假房产证的封皮有明显区别。真房产证的封皮使用的纸张是进口涂塑纸，而大多数假房产证采用的都是镀膜纸。镀膜纸的塑料镀膜很容易就能撕下来，据此可以判断是不是假房产证。另外，通过对比封面的美观程度也可以辨别是不是假房产证。真房产证的封面字迹清晰、外表精美。

第八，真假房产证的封面里页是不一样的。真房产证的封面里页中有一个五瓣叠加团花，由土红、翠绿两色细纹组成，线条流畅，纹理清晰。而假房产证则印制粗糙、线条刻板，很容易就能看出来。另外，在房产证的发证机关盖章页上，真房产证具有上下左右均等宽对称的咖啡色花纹边框，花纹细腻、清晰，假房产证的工艺水平根本达不到这种程度。

我们讲述的是有关房产的产权认证，延伸到其他产权领域都是一样的，产权确认程序都比较复杂。

10.2.2　可追踪的区块链产权变更

房地产行业正在尝试将区块链技术运用到房屋产权交易环节。未来区块链

有可能为地产行业提供全面立体的支持，改造整个行业交易模式。

Ubitquity LLC 是一家美国房地产区块链公司。2016 年上半年，该房地产区块链公司对外宣布正在研发适用于房地产行业的文件安全存储区块链平台。

Ubiquity LLC 联合创始人、CEONathan Wosnack 表示，区块链技术的应用将会极大地降低文件编程的风险。在美国，每年因为欺诈性转移问题带来的损失达到 10 亿美元，一些人采用非法手段冒充房屋所有者拿到了金融机构的贷款。因此，区块链技术将会推进房地产行业人员更好地合作并有效减少诈骗案件。从具体操作上看，区块链的公开透明的特性可以减少产权搜索时间，提高保密性。

用区块链技术解决房地产行业欺诈案件频发的问题，我国企业也在行动。鑫苑集团是中国第一家在美国纽约交易所上市的地产集团。2016 年 7 月 10 日，鑫苑集团发布区块链房产数字化应用成果——房易信。该房产数字化平台是鑫苑集团与科技巨头 IBM 进行战略合作的成果。

IBM 提供的智能合约技术和区块链技术是房易信平台的底层技术，在此基础上，鑫苑集团负责搭建上层模块，包括房地产信息数据库、交易流通系统、房产估值系统、风险控制等。房易信平台致力于成为未来房地产金融科技领域的基础设施应用，广泛对接投融资机构、征信机构、商家、消费者等机构和群体。

区块链对于解决房地产交易中出现的房产证明以及交接时的信息不对称问题，可谓是对症下药。在房地产交易市场，区块链可以创建一个公开透明，难以伪造的文档来证明交易。当有人试图制造假的交易文件时，区块链将证明该文件的拥有者不是他，从而帮助他人识别诈骗。

与此同时，区块链技术使得产权变更更易于追踪。金融机构可以据此查询相关的房产资源情况、抵押贷款公司信誉度等，大大降低了成本。

在房屋租赁市场，区块链也有用武之地。基于区块链技术的身份及信誉管理系统一旦建成，共享经济的普及就不再遥远。在这个身份及信誉管理系统里，主客身份信息的认证变得更加安全，信誉信息的准确度更高，主客双方的使用便捷度和安全性也得到了进一步提升。另外，区块链技术还有助于建立起一个不可篡改的评论生态环境，只有那些附上入住 / 支付记录并提供数字签名的真

实用户才能发表评论，评论真实性因此有了极大保障。

2016 年 4 月，格鲁吉亚共和国公共登记处（National Agency of Public Registry）、比特币挖矿公司 BitFury 以及秘鲁知名经济学家赫尔南多·德·索托（Hernando DeSoto）宣布合作开展土地所有权登记项目的研发和设计。

该项目在全球范围内引起了轰动，区块链爱好者对于用区块链进行土地所有权登记满怀期冀。格鲁吉亚是一个进步和创新的国家，因为近几年来的反腐败斗争而受到关注。

在美国、欧洲等国家，财产所有权登记基本上已经普及开来，但是从全球范围来看，很多国家依然缺少产权登记。秘鲁首都利马自由和民主研究所的主任 De Soto 估计，这笔非生息资产的总价值超过了 2 000 万亿美元。

在合作签约仪式上，项目合作方在格鲁吉亚科技园签下了协议。BitFury 作为第一家入驻该科技园的公司，买下了一块 200 万平方英尺的私有土地，用以建立其大型数据中心。

BitFury 的创始人兼 CEO 瓦列里·瓦维洛夫说："我们启动这个产权登记项目的目的是帮助格鲁吉亚公民在区块链上登记资产。而选择区块链技术的原因是它可以帮助我们解决三大问题。首先，它能增强数据的安全性，防止篡改；其次，通过区块链登记产权有助于审计员实时审计，提升审计效率，由原来的一年审计一次转变为每十分钟审计一次；最后，它可以减少登记时的摩擦和登记成本，因为未来人们可以用智能手机完成登记，区块链将提供公证服务。"

格鲁吉亚共和国公共登记处主席 Papuna Ugrekhelidze 说："通过搭建基于区块链技术的土地所有权登记项目，格鲁吉亚可以向世界展示，我们是现代化、透明、无腐败的国家。我们将会引领世界改变土地所有权的登记方式，为全世界人类社会的繁荣奠定基础。"

赫尔南多·德·索托（著有《资本的秘密》一书）是一位秘鲁经济学家，他在所有权方面的研究获得了众多奖项，因此声名远播。他说："在全球 73 亿人口里，仅拥有合法、有效和公开财产所有权的人数只有 20 亿；如果所有财产没有合法记录，那么用作抵押品获得信用贷款是不可能的，也无法作为资产转移凭据获得投资。即使财产存在所有人，可是如果没有充分记录保障，就

不能用作资产和信用。”

所有权登记问题还遏制了商业发展。赫尔南多·德·索托说：“对于雀巢、好时或亨氏公司来说，要想在加纳买几百万亩的土地，首先必须要知道向谁购买，这就涉及所有权登记问题。”

在当前的所有权登记制度下，在格鲁吉亚完成一笔土地买卖，只需要随便找一个公共登记机构，支付 50 ～ 200 美元的费用。整个流程在一天之内可以完成。当然，你对交易公证速度的要求越高，需要支付的费用就越高。如果格鲁吉亚的试点项目研发成功，土地买卖双方只需要花费 0.05 美元或 0.1 美元就可以完成一笔交易。

BitFury 副董事长乔治·科瓦德兹（George Kikvadze）说：“我们希望取得的结果是，公民用手机应用就可以转移资产，而且这些都与区块链上的代币相对应，发生交易摩擦的概率将会非常低。”

乔治·科瓦德兹还说：“格鲁吉亚政府非常支持我们的项目，不仅总理支持这个试点项目，技术小组也提供了很多支持。很多年前，格鲁吉亚政府就对该领域进行了改革，因此对接下来的工作很感兴趣。所以说，在一个完全互信、互相学习的环境下工作更加轻松。相比那种不断与腐败官员和心怀叵测的人作斗争的环境，这种合作的氛围可以使我们获得更多成效。”

如果该试点项目最终成功，将会搭建相关方案并拓展至所有土地所有权登记系统运作不够完善的国家。

通过分析区块链在国内外房地产市场的应用，我们总结了区块链技术对房地产交易过程的改变，主要包括三个方面，内容如图 10-2 所示。

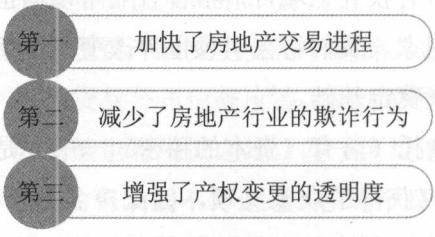


图 10-2　区块链技术对房地产交易过程的改变

第一，加快了房地产交易进程。众所周知，房地产交易流程是比较复杂的，

各个国家的不同的附加限制以及转让成本更是降低了房地产交易速度。区块链技术的使用将会加快与财务有关的交易环节。

目前，大部分房地产买卖交易都是通过第三方中介机构进行的。虽然，这种交易方式可以保证双方财产与资金安全，降低欺诈风险，但是费用成本较高，占财产总价值的 1% ～ 2%，而且还延长了交易进程。使用区块链技术后，第三方中介机构的角色将会消失，区块链分布式账本本身就可以保障交易安全，从而加快交易进程。

第二，减少了房地产行业的欺诈行为。买卖双方通过第三方中介完成房地产买卖交易的主要原因是降低欺诈风险。而区块链可以替代第三方中介的作用，锁定买方的资金，同时验证卖方的数字产权。区块链的共识机制可以轻易识别伪造的所有权文件以及虚假广告，并且在系统里直接链接到唯一的财产，发生欺诈行为的概率几乎为零。

第三，增强了产权变更的透明度。大部分人买房都是贷款购房，全款购房的较少。然而，到银行贷款的流程也比较烦琐。区块链技术可以改变这种现状。在区块链上，人们可以将自己定义为买方，申请贷款时，信用记录以及收入等信息会立即被核实，省去了前往银行、律师事务所及地产代理机构办理各种手续的环节。

对房主来说，房子本身拥有数字身份，只有自己拥有唯一的密钥，从而轻松证明自己对房产的所有权。另外，房屋交易历史记录、维修和翻新记录以及相关的预计成本等记录在区块链上。这样一来，贷款手续以及所有权的转移将无缝连接，甚至可以在同一天内完成。

区块链在房地产领域的应用真是恰到好处，基于区块链技术的信息共享可以避免房地产交易过程中的欺诈行为，减少整个社会的财产损失，并提高房地产行业的运行效率。相信未来，区块链技术会在房地产市场得到进一步的应用，甚至可能替代房地产中介的职能。

10.2.3　杜绝洪都拉斯的土地所有权纠纷

洪都拉斯是一个经常发生土地所有权纠纷的国家。为此，洪都拉斯政府已

经与区块链链公司展开合作开发使用区块链技术记录土地所有权注册的方法。调查记者凯文·卡希尔（Kevin Cahill）著有《谁拥有不列颠》一书，书中指出，英国有一半的土地处于未登记状态。不仅是洪都拉斯还有英国，土地所有权纠纷几乎是任何国家都发生过的事情，下面我们看看洪都拉斯发生的一个房屋所有权纠纷范例。

2009年的一天，洪都拉斯警方突然闯入Mariana Catalina Izaguirre的家里，让她立即离开。Mariana Catalina Izaguirre非常惊讶，不知所以然，因为她已经在这个家里住了三十多年。

为了证明这个家是自己的，Mariana Catalina Izaguirre将自己家里存放的政府开出的房屋证明拿出来给警察看，然而警察告诉她："来自当地政府房屋委员会的资料显示，该房屋属于另外一个人，而这个'房主'向法院申请了驱逐令。"最终，Mariana Catalina Izaguirre被迫离开了自己的家。

这是发生在洪都拉斯真实的事情，很多人听闻此事后只感觉非常荒唐。事实上，因为登记不详或记录丢失，像这类不公平的事情在全球都很普遍。房屋以及土地所有权保障的缺失便是不公正的源头，也导致了利用房屋或土地作为抵押物进行融资等变得异常困难。

这就是洪都拉斯政府与Factom公司（为基于区域链的土地登记提供原型的美国创业公司）合作开发使用区块链技术记录土地所有权注册的方法的原因。同时，希腊也对Factom公司产生了兴趣，因为希腊没有合适的土地登记政策，90%以上的土地在绘出的地图上都是错误的。

赫尔南多·德·索托认为，发展中国家的发展之所以非常缓慢，是因为财产所有权界定不够明晰。如果连财产属于谁都无法判定清楚，那么投资行为就不会出现，经济发展必将受到限制。想象一下，当财产所有权清晰以后，人们就能够交易，而交易是繁荣的基础。

区块链的支持者认为，区块链技术能够解决财产所有权的界定问题。它通过均等的节点权力和义务分配，创造了一种解决彼此之间不信任的更公正的记账方式。一旦财产的所有权明晰，基于合伙或者财产的权利也就可以确定了。

于是，我们所处的发展阶段将会超越所有权，通过智能合同来解决财产纠

纷问题。以一个人拥有债券为例，当智能合同制定之后，如果没有满足一些条件就会产生相应的利息、在规定时间内偿还或者发生罚金等。这些条款能够在区块链上被编码，所有相应的行为都是自动化处理的。

在财产所有权方面，区块链很可能会完成银行家、律师、管理员和注册机构的工作，而且标准更高，成本更低廉，极大地降低财产所有权发生纠纷的可能性。

10.3
公证通 Factom 白皮书

Factom 区块链公司曾于 2013 年发布一份白皮书，大致意思就是他们构思了一种概念型网络框架，这个新框架可以确保并提高留存在比特币区块链里的交易记录、文件及其他一些重要数据的准确性。截至 2017 年，这份白皮书被各大公司、机构研读。

10.3.1　Factom设计目标——真实地记录一切

利用比特币以加密的形式来确保信息准确性这一概念在过去几年里不断被完善。而 Factom 公司则提出一种依托比特币系统的新系统，增强比特币系统里的加密认证信息的透明性与开放性。

Factom 致力于使用区块链技术来革新政府部门和商业社会的数据管理和数据记录方式。Factom 的目标是创建并维护一个永久存储且不可篡改的、基于时间戳记录的区块链数据网络，从而实现真实记录的管理，减少进行独立审计的成本和难度。

当前的比特币区块链已经改变了交易记录的方式，开发商们纷纷开始研发基于比特币区块链上的应用程序。然而，比特币受制于最初的设计权衡，这给开发商带来了三个核心约束问题，内容如图 10-3 所示。

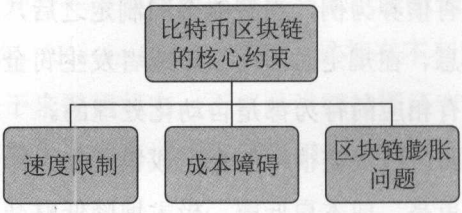


图 10-3　比特币区块链给开发商带来的核心约束问题

首先是速度限制。比特币的分布式设计和工作量证明的共识机制导致比特币网络生成一个新区块的时间长达 10 分钟。有的开发商需要开发具有更高安全性的应用，所以存在许许多多个确认。比如说，等待六次确认是一个常见的要求，而这需要的时间可能会比一个小时还要长。

其次是成本障碍。比特币的交易价格始终在波动，就像起伏不定的股票一样。如果比特币的价格上涨，那么交易成本也会跟着上涨。对于大型应用程序来说，管理的数字交易数据规模大，那么交易成本就是一个非常大的障碍。除此之外，区块大小的限制、奖励减半等多种因素都会引起交易费用的增加。

最后是区块链膨胀问题。比特币的网络规模是最初就已经决定好的。当时，创始人中本聪对网络数据流量进行了限制，上限设为每秒交易 7 次左右，区块大小上限为 1M。随着比特币越来越受追捧，这些限制导致了严重的网络阻塞。任何应用程序若想要使用区块链写入和存储信息都将会增加流量。这一问题使各方不得不寻求增加区块大小限制。

Factom 旨在创建速度更快、成本更低、无膨胀的区块链协议解决比特币区块链的三大核心约束问题。Factom 构建了一个标准的、有效的、安全的基础，这将使基于协议之上的应用程序运行速度更快、成本更低，并且不会造成区块链膨胀。可以说，Factom 协议为应用程序提供的功能和特性已经超越了虚拟货币。

Factom 生态系统建成之后，用户账号和公证通币（Factoids）将会被激活，Factoids 承担交易货币的角色。Factom 系统和比特币之间的互动过程为：

第一，应用程序开发商使用公证通币购买数据条目信用（Entry Credit）；第二，应用程序记录数据条目；第三，Factom 服务器创建条目区块和目录区块；第四，Factom 将目录区块的哈希值锚定到比特币区块链。

那么，Factom 系统是如何安全地记录数据条目的呢？比特币原本的功能仅限于其货币属性之内的事件记录的功能，而 Factom 扩展了比特币的功能。Factom 设置了用于永久记录数据条目的最小规则集，让开发商的应用程序独立执行大多数的数据验证任务，Factom 仅仅强制实施那些通过协议交易公证通币、购买条目信用的验证，并确保条目正确付款和记录。

Factom 创建了一些规则，用于激励运行网络和内部的一致性，但是这种规则无法检验用户记录信息本身的真实性和有效性。另外，Factom 对比特币交易采取了一定的限制，要求比特币交易必须从一组输入值集合映射到一组输出值集合。在一定的签名下，只要输入值集合满足输入值条件，系统输入的有效性就可以得到保证。一旦这个验证过程可以实现自动化，那么审计过程就变得更加容易。

举例来说，Factom 通过记录房地产转让发生的那一时刻确保房地产的产权转让事件被记录。现实世界里的房地产产权转让规则和过程都非常复杂。房地产购买者不同，地方管辖机构的要求就可能大不相同。也就是说，外国人、农民或城市居民购买房地产的限制条件是不一样的。另外，房地产的房屋价格、地段位置或建筑类别等不同属性都可能使房地产被归为不同的类别，而每个类别反映到智能合约的验证和执行上也都有自己的规则。

情况的复杂要求所有权转移验证需要多个加密签名，否则就无法保证有效性。而 Factom 另辟蹊径，不验证房地产所有权转移是否有效，而是记录房地产所有权转移和交易是否发生。

Factom 服务器是如何验证数据条目的呢？按照时间顺序来说，Factom 将这个过程分为记录条目和审计条目的有效性。

首先是记录条目。Factom 服务器接收数据条目后会把它们装入到不同的区块，并修复条目的顺序。10 分钟后，该条目的顺序被插入到比特币区块链的一个锚定，而后永久存储，不可篡改。这一功能的实现依赖于 Factom 为 10 分钟内收集的数据创建哈希值，然后将哈希值记录到比特币区块链上。

其次是审计条目的有效性。条目审计是一个独立过程，可以选择依靠信任第三方或者不依靠信任第三方来进行。

如果选择依靠信任第三方，轻型应用可以找一个称职的审计师。每当项目

被输入到系统中后，审计师将验证输入是否有效，并提交上自己的加密签名条目。附上加密签名表示该数据条目已经通过了审计师认为必须做的几项检查。依然是之前所说的房地产案例，审计师会仔细检查财产转移是否符合地方管辖机构的标准。在这种方式下，审计师将会公开证明财产转移是有效的。

如果选择不依靠第三方信任，这种情况与比特币网络类似。也就是说，只要有一个数学定义像比特币网络一样完美的系统，就可以实现审计过程程序化。在这一系统的基础上，应用程序只需要下载相关数据，然后进行自我审计和审核过程，建立起对系统的感知。

要把这些由客户端独立验证的协议转移到 Factom 上仅仅是一个如何真实记录并保存数据交易的问题。与比特币比起来，交易协议在 Factom 上没有什么不同，依然是永久存储、不可篡改。唯一的不同是信息在 Factom 上更容易表达，而不必以特殊形式编码然后再嵌入比特币的交易信息中。

10.3.2 解决的问题——“证明否定”

房产登记、土地登记、比特币以及其他众多系统都需要解决一个根本问题，即“证明否定”。也就是说，他们需要证明一个东西已经被转移给某人，而且没有被转移给其他所有人。无界系统里不存在否定证明，但有界系统里可以实现。

首先看土地所有权记录系统。假设土地所有权系统规定，土地转让必须在政府登记才有有效，未记录的转让是无效的。那么，一个人想要检查一块土地的产权归属只需要去政府登记处就可以。政府记录可以证明这块土地归属于谁，而且不被第三方拥有。如果产权登记不是必须的，那么政府登记处只能证明那些被登记的土地产权归属于谁。而且，在这种情况下，私人转让很可能存在，政府记录无法代表全部的转让情况。

以比特币为代表的数字货币系统也是类似的。比特币系统将交易数据存在的地方限制在区块链上。如果比特币区块链里不存在某个交易，那么它在比特币协议下就不存在，因此不存在双重交易的问题。

在上述两种情况下，否定证明可以在一定的限定下得到证明。但是，现实

世界是极其复杂的，而 Factom 则针对精确的数字资产以及物质世界中复杂的现实情况解决证明否定的问题。

在 Factom 系统中，数据的分类是有层次结构的，而 Factom 只把数据条目记录在链中。如此一来，在 Factom 的执行协议中，众多用户定义的链不是相互依赖的关系，因此也不会像比特币交易一样存在双重支付的问题。与比特币系统将全部数据合并成一个总账相比，Factom 将各个数据条目放在多个链当中，尽量让应用程序在较小的空间内搜索数据。

比如，通过 Factom 系统管理土地转让的应用程序仅仅是使用某个链来记录，同时安全地忽略其他链上的条目数据，也就是说，那些用于停车场监控记录的链就不需要更新。如果政府法院判决需要变更土地转让记录，那么与之相关的链都会被更新，用来反映判决结果。但是，数据一旦被更改，更改的历史就永远不会消失，即使这样的数据更改从法律或者其他角度来说是无效的。

尼克·萨博在论文《安全产权与所有者权限》中的一个观点就是："尽管暴徒依然可以通过暴力掠夺物质资产，但是持续存在的真正的所有权记录将是盗用者的眼中钉。"

综上所述，Factom 是在比特币区块链协议的基础上构建的一种分布式的、匿名的数据协议。Factom 将比特币区块链技术的应用范围拓展，赋予了比特币应用到无限场景中的能力。另外，持有加密货币并不是使用 Factom 系统功能的必备条件。

比特币区块链代表的本质创新和技术突破是一个分布式的、不可篡改的分类总账技术。而无数用户和开发者的梦想是将分类总账技术的诚实性和不可欺诈性应用到现实生活中。Factom 是一种解决方案，它基于区块链技术创造了新的分类总账，从而把区块链技术的优势带进了现实生活中。

10.3.3　公证通币430万枚价值54万美元

2015 年 4 月，Factom 公司对外宣布，通过销售 430 万枚公证通币共获得了超过 54 万美元的收入，并对支持者表示感谢。据悉，Factom 公司销售公证通币获得的资金将会用于开源项目的后续开发，加速软件的研发以及发布。

根据公证通白皮书：“Factom 创建并维护了一个永久存储且不可篡改的、基于时间戳记录的区块链数据网络，从而实现了真实记录的管理，减少进行独立审计的成本和难度。商业社会和政府部门可以利用 Factom 简化数据记录的管理，记录商业活动，并解决数据记录安全性和符合监管的问题。”

在公证通发布公测版后，公证通币持有者就可以使用并交易公证通币了。Factom 公司创始人兼 CEO 保罗·斯诺（Paul Snow）称：“比特币社区的热情让我们感到受宠若惊。我们将会持续改进公证通的 API，并为软件开发者提供整合公证通的教程。”

Factom 公司的发展是引人注目的，受到投资人的青睐也不足为奇。2015 年 7 月份，Factom 公司通过 BnkToTheFuture 众筹服务平台出售了部分股权，拿到了 110 万美元的融资。

2015 年 10 月，Factom 公司获得了来自 Kuala Innovations 公司的 40 万美元种子资金。Kuala Innovations 公司以每股 1 美元的价格购买了 Factom 公司 3.64% 的股份，共计 40 万美元。此轮融资中，Factom 公司的估值达到 1 100 万美元。

Kuala Innovations 公司联席董事长吉姆·梅隆（Jim Mellon）在陈述中表示：“Factom 是极具潜力的，它将会从根本上解决企业业务中存在的商业问题。”吉姆·梅隆还说：“随着销售的增长，广泛的开发者网络会集成更多的应用，董事会相信，由 Kuala Innovations 公司投资的这轮种子轮，对于 Factom 预期在 2016 年上半年完成的 A 轮融资来说，具有很大的意义。”

Kuala Innovations 公司对 Factom 公司的投资是 Kuala Innovations 公司第二次投资比特币和区块链公司。2014 年 12 月，Kuala Innovations 公司还为比特币微支付创业公司 SatoshiPay 提供了 16 万欧元（18.3 万美元）的资助。

尽管 Factom 公司拿到的 A 轮融资不是在 2016 年上半年，但也相差没有几个月。2016 年 10 月，Factom 公司获得由硅谷风投教父蒂姆·德雷珀（Tim Draper）领投的 420 万美元 A 轮融资。

Block chain

第11章
区块链发展趋势分析与预测

2016年年初，华尔街巨头投资银行高盛发布报告表示，区块链技术已经做好准备要颠覆这个世界。此前，高盛已经和中国IDG资本联手向区块链创业公司Circle Internet Financial投资5 000万美元。自2016年以来，不仅是高盛，金融界其他巨头也纷纷向区块链技术抛出橄榄枝。投资者们为什么蜂拥而至进入区块链领域？是因为区块链极具想象空间。区块链虽然诞生于比特币，但是抛开比特币不说，区块链具有的发展机会更多。

practice

11.1 区块链技术发展趋势

区块链有一个非常好的特性，它不会直接抛弃现有的基础设施，而是在小规模、小面积改动的基础上引进技术。可以说，区块链的兼容性是非常好的。基于这种兼容性，区块链与大数据、物联网、人工智能等新兴领域深度融合。

11.1.1 区块链与物联网、大数据、人工智能深度融合

在当前的互联网时代，技术是基础、场景是土壤、金融是催化剂，三者只有相互融合才能推动时代发展。而且技术的融合成本也是一个问题。

技术改革一般都会带着历史的遗留成本的，不可能从零开始做。以接受改革的金融企业为例，它在改革过程中的数据以及业务流不会中断。而在区块链受到众人关注之前，物联网、大数据以及人工智能就已经是科技领域的三个巨头，已经渗透到人们的生活中，这就要求区块链与大数据、物联网以及人工智能可以很好地融合在一起。

在区块链尚未诞生之前，物联网可理解为大数据的来源，人工智能作为大数据的后台工具，然后通过大数据驱动业务变革。现在，区块链是如何与这三种技术融合的呢？

首先看区块链与物联网。物联网就是物物相连的互联网，实现设备与设备、系统与系统之间的民主和独立。处于物联网中的设备爆增是一种必然趋势，有可能达到千亿甚至万亿或者更多。如此庞大的网络以中心化的代理通信模式或者服务器 / 用户模式去管理的话，基础设施的投入以及维护成本是无法估量的。2015 年 5 月发生的支付宝杭州萧山机房光纤挖断事件就说明了这一问题。

即使成本问题可以顺利解决，中心化的云服务器本身依然是一个瓶颈和故障点，这个故障点有可能会颠覆整个网络。从物联网的当前环境看，云服务器的这种颠覆性作用还没有明显表现出来，但是当人们的健康和生命对物联网的依赖越发明显时，这就显得尤为重要了。

因为我们无法构建一个连接所有设备的单一平台，无法保证不同厂商提供的云服务是可以互通而且相互匹配的。而且设备间多元化的所有权和配套的云服务基础设施将会使机对机通信变得异常困难。

区块链技术破解了物联网的超高维护成本以及云服务器带来的发展“瓶颈”。区块链可以通过数字货币验证参与者的节点，同时安全地将交易加入账本中。交易由网络上全部节点验证确认，消除了中央服务器的作用，自然就不需要为维护中央服务器而付出超高成本。

区块链与物联网的结合可以构建一个物联网网络去中心化的解决方案，从而规避很多问题。采用标准化 P2P 通信模式处理设备间的大量交易信息可以将计算和存储需求分散到物联网网络中存在的各个设备中，这样可以避免由于网络中任何单一节点失败而导致整个网络崩溃的情况发生。然而建立 P2P 通信的挑战非常多，最大的挑战就是安全问题。

物联网安全不仅仅是保护隐私数据这么简单，还需要提供一些交易验证和达成共识的方法，防止电子欺骗和盗窃。那么，区块链带来的解决方案是什么呢？

区块链为 P2P 通信平台问题提供的解决方案是一种允许创建交易分布式数字账本的技术，这个账本由网络中所有的节点共享，而不是交给一个中央服务器存储。

区块链分布式账本是防篡改的，恶意犯罪分子根本没有机会操纵数据。这是因为分布式账本不存在任何单点定位，没有可以被截断的单线程通信，可有效的避免中间商的攻击。区块链真正意义上实现了可信任 P2P 的消息传送，并且已经通过以比特币为首的数字货币证明了自己在金融业的价值，不利用第三方中介就可以完成 P2P 支付服务。

研究表明，区块链将使物联网中的设备实现自我管理和维护，省去中央服务器高昂的维护费用，降低物联网设备的后期维护成本。可以说，区块链与物联网的结合是天作之合，有了物联网，区块链获得了更高质量的数据来源；有

了区块链，物联网由中心化管理变成自管理。

再看区块链与大数据。区块链是一种通过去中心化和去信任的方式集体维护一个可靠数据库的技术方案，这也注定了区块链与大数据联系在一起是必然的趋势。甚至可以说，区块链的诞生是对大数据的重构。下面从五个方面看区块链与大数据的融合，内容如图 11-1 所示。

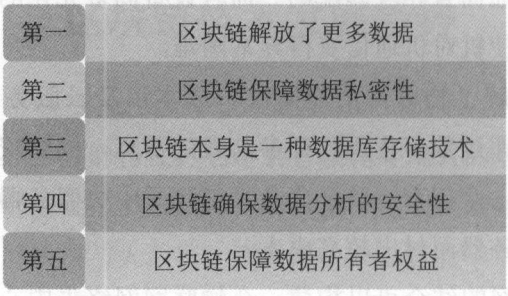


图 11-1　区块链与大数据的融合

第一，区块链解放了更多数据。区块链基于可信任性、安全性和不可篡改性解放了更多数据。例如，区块链推进了基因测序大数据的产生。区块链测序可以使用私钥限制访问权限，这种方式规避了法律对个人获取基因数据的限制。另外，区块链还使用分布式计算资源完成测序服务，成本非常低。区块链的安全性为基因测序工业化提供了解决方案，推进了全球规模的测序产生大数据，最终实现了更多数据的解放。

第二，区块链保障数据私密性。全球大量高密度、高价值的数据都掌握在政府手里，包括人口数据、医疗数据等。政府数据开放共享是必然趋势，将会极大地推动整个社会经济的发展。但是，政府数据开放共享面临的一大难点和挑战是保护个人隐私不受侵犯。

区块链为政府数据在保护个人隐私不受侵犯的前提下开发共享提供了解决方案。这一解决方案主要利用了基于区块链技术的数据脱敏技术。数据脱敏技术指的是通过哈希处理等加密算法在不访问原始数据的情况下运算数据。

例如，基于区块链技术的英格码系统（Enigma）就是通过这种方式实现数据共享的。通过英格码系统，公司员工可以开放可访问其工资信息的路径，而且无须担心他人获知自己的工资信息。当系统计算出群内平均工资，每个参与

者都可以据此分析出自己在群体内的相对地位，但是无法获知其他成员的工资。

第三，区块链本身是一种数据库存储技术。一般来说，数据发展经过三个阶段。在第一阶段，数据是无序的，而且没有经过充分检验；在第二阶段，大数据兴起，通过人工智能算法进行质量排序；在第三阶段，数据采用区块链机制获得基于互联网全局可信的质量。正是区块链能够让数据进入第三阶段。

当前的大数据还处于非常基础的阶段，而区块链本身就是一种不可篡改的、去中心的、人人都可以参与记账的数据库存储技术。区块链将会使得数据的质量获得前所未有的强信任背书，也使大数据的发展进入到一个新时代。

第四，区块链确保数据分析的安全性。大数据因为数据分析才有了价值。在进行数据分析时，有效保护个人隐私和防止核心数据泄露是首先需要解决的难题。例如，随着指纹数据分析应用和基因数据检测与分析手段的普及，众人开始担忧，一旦个人健康数据发送泄露，后果非常严重。

区块链与大数据的结合将保证数据分析的安全。区块链可以通过多签名私钥、加密技术、安全多方计算技术保证只有被授权者才可以访问数据，而且进行数据分析时不能访问原始数据。这样个人健康数据既可以提供给全球科研机构、医生共享，也可以保护数据的私密性。这一解决方案的提出将为未来解决突发疾病、疑难疾病带来极大的便利。另外，区块链上的数据质量极高，可以减少数据挖掘分析中数据收集和清洗的成本。

第五，区块链保障数据所有者权益。区块链的诞生保证了数据生产者的数据所有权。对于数据生产者来说，区块链可以记录并保存有价值的数据资产，而且这将受到全网认可，使数据来源以及所有权变得透明、可追溯。

一方面，区块链能防止中介拷贝用户数据的情况发生，有利于可信任的数据资产交易环境形成。数据与传统意义上的商品有很大不同，具有所有权不清晰、可以复制等特征，这也决定了中介中心有条件、有能力复制和保存所有流经的数据，这事实上侵犯了数据生产者的数据所有权。这种情况是无法凭借承诺消除的，也构成了数据流通的巨大障碍。当大数据遇上区块链，数据生产者的数据将得到保护，中介中心无法拷贝数据。

另一方面，区块链为数据提供了可追溯路径。在区块链上，各个区块上的交易信息串联起来就形成了完整的交易明细账单，每笔交易的来龙去脉都会非

常清晰，如果人们对某个区块上的数据有疑问，可以回溯历史交易记录判断该数据是否正确，对该数据的真假进行识别。

当数据在区块链上活跃起来，大数据也将随之活跃起来。

最后看区块链与人工智能。人工智能（Artificial Intelligence）是计算机科学的一个分支，是研究、开发用于模拟、延伸和扩展人的智能的理论、方法、技术及应用系统的一门新的技术科学。人工智能试图了解智能的实质，并生产出一种新的模拟人类大脑做出反应的智能机器。机器人、语言识别、图像识别、自然语言处理和专家系统等都属于人工智能领域的研究。

区块链 P2P 的验证方式实质上是一种基础协议，是分布式人工智能的一种新形式。区块链很有可能为人工智能构建一种全新接口和数据共享模式。另外，区块链与人工智能有着相同的根与脉络，一个是算法革命，另一个是共享经济模型。

区块链目前还是一个早期的新兴市场，突破传统行业是一件困难的事情，可以从物联网、大数据、人工智能这些新兴的科技领域开始。只有先易后难，首先完成一些案例积累，才能突破更多的场景，改变整个世界。

11.1.2 区块链为智慧城市提供原动力

什么是智慧城市呢？自“智慧城市”概念诞生以来，国内外相关企业和研究机构、专家等纷纷对其进行定义和研究。智慧城市的定义主要包括下面三个核心点。

首先，智慧城市建设的主线是信息技术应用。智慧城市是城市信息化的高级阶段，离不开信息技术的创新应用，而信息技术应用主要体现为物联网、云计算、移动互联和大数据等新兴热点技术。

其次，智慧城市包含诸多要素，各要素之间相互作用。智慧城市是一个复杂系统，包含信息技术以及其他资源要素。信息技术以及各资源要素优化配置并共同发生作用，使城市运行越来越智慧。

最后，智慧城市是城市发展的一种新模式。政府、企业和个人是智慧城市的服务对象。智慧城市的最终结果是变革、提升和完善生产与生活方式，让人

们的城市生活越来越美好。

现如今，智慧城市已经是国家级的战略规划。作为经济转型、产业升级、城市提升的新引擎，智慧城市体现了更高的城市发展理念和创新精神，有助于提高民众生活幸福感、企业经济竞争力，实现城市可持续发展的目的。

相关资料显示，我国最早建设智慧城市的时间为 2012 年。2013 年年初，我国公布首批智慧城市试点共 90 个；同年 8 月 5 日，住房城乡建设部公布第二批 2013 年度 103 个国家智慧城市试点。截至 2016 年 6 月，全国智慧城市试点一共有 290 个，500 多个城市已明确提出构建智慧城市相关方案。

随着国家政策的大力推动以及逐渐落地，智慧城市建设受到越来越多人们的认同和欢迎。与此同时，智慧城市建设发展迅速，智慧城市概念类公司的发展也进入快车道。

截至 2016 年 10 月，全国新三板智慧城市概念类挂牌公司共有 65 家，其中创新层挂牌公司有 13 家，基础层公司数量为 52 家。2013—2016 年的 4 年时间里，65 家公司共发起 66 次定向发行，募集资金达到 18.5 亿元。

2013 年，这 65 家新三板智慧城市概念类挂牌公司成功融资 1 次、2014 年成功融资 4 次、2015 年成功融资 29 次、2016 年 1 月 1 日—9 月 30 日成功融资 22 次。据统计，在新三板新科技概念类 17 家公司中，智慧城市概念类挂牌公司以 18.5 亿融资额排名第五，前四名分别是云计算 53.6 亿元、虚拟现实 37.3 亿元、物联网 36.8 亿元、大数据 36.2 亿元。

虽然现在智慧城市概念仅以智慧小区和智慧家庭的形式落地，还需要通过融资获得快速发展，但是智慧城市概念类挂牌公司在新科技概念类公司融资中排名靠前，足以说明智慧城市概念类企业受到了投资人的追捧。可以预见，智慧城市概念类企业融资成功次数与获得融资金额将会逐年递增。

智慧城市概念的火热使业绩不好的智慧城市概念类挂牌公司也能成功融资。以航天汇智为例，航天汇智是为智慧城市公共安全和应急管理的信息化建设提供包括综合应急及行业专项应急在内的整体解决方案、产品和增值服务的企业。2016 年 10 月 28 日，航天汇智在新三板公开发行股票 115.67 万股（全部为无限售条件股份），发行价格为 9.16 元每股，募集资金 1 059.54 万元。

本次募集资金主要用于扩大生产经营，开设区域子公司，增强研发能力投

入项目研发，增强销售能力建设，销售市场体系。

参与航天汇智此次定向发行的投资人有3个，包括认购500万元的河南中证开元创业投资基金管理有限公司——中证和璞新成长1号基金、认购500万元的深圳益友远投资有限公司以及认购59.54万元的自然人投资者郑世纲。

然而，航天汇智的业绩并不乐观。据2016年半年报显示，航天汇智的净利润同比亏损严重，为-6 422.56%。在新三板智慧城市概念股中，航天汇智的净利润亏损率最高。

2014年，我国政府首次将智慧城市概念纳入国家级的战略规划中，随后更是大力推动智慧城市的建设。或许这就是智慧城市概念类挂牌公司虽然业绩不佳却能得到投资人的重点关注并且成功融资的原因之一。

随着投资人对智慧城市概念类挂牌公司的重点关注，继腾讯、阿里加入智慧城市的发展争夺战，A股上市公司也加入其中。

2016年3月13日晚间，A股上市公司格林美发布《格林美：关于对外投资的公告》，公告称："为了实现互联网与智慧城市、环保城市的大融合，构建'互联网+智慧云+环保云'的城市管理新模式，积极参与'互联网+'的时代大潮，依据格林美股份有限公司（以下简称'公司'）与江苏广和慧云科技股份有限公司（以下简称'慧云股份'）控股股东常熟慧云企业管理有限公司、孟庆雪签署的《股权转让协议》，公司收购淮安繁洋企业管理有限公司（以下简称'淮安繁洋'）79.85%股份后，通过淮安繁洋继续对慧云股份增持，使公司控股子公司淮安繁洋持有慧云股份的股份达到20%。

"鉴于此，公司在完成收购淮安繁洋79.85%股份的基础上，公司控股子公司淮安繁洋与慧云股份签署了《股票认购合同》。根据认购合同，淮安繁洋拟以现金方式认购慧云股份本次新发行股票中1 647.30万股，发行价格为每股人民币13.33元，认购总金额为人民币21 958.509 0万元。本次认购完成后，淮安繁洋将持有慧云股份3 800.987 2万股，持股比例为20%。"

智慧城市不仅是我国的投资焦点，也是全球投资和关注的焦点。据市场研究机构Pike Research预测，到2020年，全球范围内的智慧城市基础设施投资将累计达到1 080亿美元。

智慧城市的建立面临一个亟待解决的问题，即如何在经济发展的同时保证

人口包容性。在解决方案的探讨中，“区块链”被人们广泛提及。如果区块链相关应用得以落地，它将会成为智慧城市的一部分，支持利用信息和网络技术来影响城市的运作。

在智慧城市里，任何联网设备都相当于传感器，包括管道、路灯、汽车、手机等。但如果网络中只存在几个少数的数据处理中心，一旦中心发生黑客入侵、服务中断等问题，整个城市都将陷入瘫痪。

在 11.1.1 小节中已经讨论过区块链对物联网的革命性影响。当基于区块链技术的物联网应用到智慧城市中时，商业区和居民区之间的网络将高效运转。全球部分地区政府及机构已经建立了一些基于区块链记录核查和审计的基础设施公司和咨询公司，目的是提供城市基础设施的连接以及实时数据智能响应方案。

畅想一下智慧城市下的生活：出门在外，智能终端帮助你轻松快捷地找到停车位；拨打急救电话，智慧医疗系统自动分析出你的位置，然后向你赶来；走进家门，智能家居自动为你打开窗帘，根据你的心情调整灯光颜色……区块链将加速这种生活的到来。

11.2 区块链行业发展前景

2016 年是区块链概念被不断验证的一年，而 2017 年，区块链技术将从实验室中走出来，进入真实的市场环境。区块链是够能够真正服务于人类生活对区块链行业来说是决定成败的因素。从浮躁到淡定，区块链行业将落到实处，在商业机构、政府和用户的共同推动下实现商业价值，逐渐形成一个交易、监管和执行成本不断降低的区块链环境。

11.2.1 这是一场降维性经济战争，财富转移已成必然

“降维”的概念来自于刘新慈的玄幻小说《三体》，讲的是太阳系之外的

高等文明发明了一种叫作“二向箔”的武器可以将太阳系从三维降到二维，在人类无法适应二维的情况下，地球文明即将毁灭就成为必然。

如今，人们发现“降维”的概念在现实生活中也非常适用，所以“降维”从科幻走向现实，被很多业内人士所津津乐道。“降维”的表述非常形象，如果人类由三维降到二维就无法生存。如果一个企业从三维降到二维同样无法生存。随着互联网的发展，很多企业发现自己失去了很多维度，对企业形成了严重的打击。

在同一个维度上竞争，要想取得胜利是非常困难的。比如，360 不会打败百度；拍拍打败不了淘宝，来往不能打败微信。因为在同一维度上，先来者具有很大的优势，而且能有一份成就的创业者总是有一些本事的。想要改变已经形成的市场格局最好的方法就是降维，然后与之竞争。

电子商务因为没有地域的限制，所以竞争优势很明显，同时也对很多传统的线下企业产生了很大冲击。在过去，任何一个商场只要开在人流量很高的地区，生意就能红火，在互联网的打击下，地域这个维度几乎不存在了。

互联网巨头对运营商采取的“降维”竞争手段更是直接有效。腾讯、微信等通过整合语音、文字和多媒体，为用户提供了一个体验优质的信息交互平台，运营商因此“降维”成一个传输管道。

由此可见，区块链对现有经济社会的打击也具有“降维”特征。在区块链技术主导的世界里，获取所有服务的渠道都处于同一个网络中，就像邮件一样采用 P2P 的方式，从而省去加入第三方平台的烦冗手续。而且，这个网络中的信息交互都是通过分布式运算引擎上运行的加密算法自动完成的，从而不会受到任何个体或组织的控制。

当前，这种去第三方平台的假设依然没有成为科技界主流的原因是显而易见的，因为其竞争对手非常强大，它们常常通过免费模式吸引用户，利用广告或者用户数据来变现，最后成为市场中的垄断巨头。然而，互联网的发展让公司、组织以及个人相互联结在一起，直接进行交易而不需要借助第三方平台逐渐有了实现的可能。

这一次，区块链最关键的技术，它将各种移动应用背后的复杂机制转变为一个更完美的系统，帮助用户预订飞机票、订车、订酒店，顺便提供几首好

听的音乐。正如 P2P 基金会的核心成员以及都柏林圣三一学院的讲师 Rachel O’Dwyer 所说：“区块链创造了一种可信的数字货币和会计系统使人们就不必向美联储这样的集中式媒介求助。”

在区块链系统里，参与者之间可能互不认识，但是大家可以共享数据、共同决策、一起建设公开透明的系统。

有一些人已经开始研发替代第三方平台的区块链解决方案，这场降维性经济战争即将爆发。在以色列，La’Zooz 针对 Uber 推出自己的共享出行应用，并将其戏称为“反 Uber”。La’Zooz 展望的未来场景是：无论你在世界上哪个地方需要坐车，你的电话就能帮你联系上附近想要与你前往同一个目的地的人。也就是说，La’Zooz 想要实现真正的“实时拼车”，而不是让用户供养一家开发了应用的出租车公司。

La’Zooz 已经在 2016 年里推出了一个安卓应用，并在以色列境内进行了一个小型试点计划。La’Zooz 的系统用自己的代币 zooz 给司机付钱，而 La’Zooz 的司机通过允许该应用跟踪自己的地理位置从而获得 zooz 币。La’Zooz 的开发者认为：“这种方法能够活跃用户，让更加广泛的人群接触到 zooz。一旦搭车业务投入运作，人们就能直接用 zooz 币来进行支付。”截至 2016 年 6 月，La’Zooz 的站点上的用户还不足 1 万人，广泛分布在世界各地，但其未来发展潜力是巨大的。

La’Zooz 的软件大部分都是由核心团队成员开发出来的，虽然还存在缺陷，但他们依旧热衷于区块链概念本身。La’Zooz 以及其他相似的项目让我们看到去平台的服务和网络的确有可能成为现实，而且我们不需要任何中心平台机构。

La’Zooz 的核心成员之一 Eitan Katchka 称：“我总是跟那些质疑我们的人说，如果回到 1993 年，你会怎么跟朋友解释电子邮件呢？”

非营利公共信托组织 XDI.org 的网络主席菲尔·温德利（Phil Windley）认为：“区块链非常复杂，这是因为人们希望通过区块链技术解决的问题也很复杂。回想一下 20 世纪 80 年代的光景，当时的人们如果想要给一些计算机建立局域网的话，面临的互联网协议也是异常复杂的。当然，与区块链相比，那些协议还是更简单一些，但是在当时的技术背景下，那就与区块链一般复杂。”

对于用区块链技术构建去第三方平台的服务系统，菲尔·温德利感到非常兴奋："区块链能够让我们把所有事物都纳入系统，而不需要任何一家公司作为中间人。当然，公司不会因此全部消失，但是有了区块链技术的应用以后，用户就可以随意更改提供商，所有的服务都能互用。代码全部都是开源的，没有任何一个特殊的组织可以独占某些资源。有了区块链以后，我们甚至有能力运营自己的服务器。"

在区块链引发的降维性经济战争中，财富首先将会向下面三个方向转移。首先是区块链行业革命性的产品或应用，包括"R3 CEV"区块链联盟、瑞波币的发行与维护公司 Ripple Labs、以太坊、小蚁和井通（北京）科技等五家国内外公司分别在交易结算、跨境支付、开源平台、非上市公司股权转让和采购平台等方面有所突破，并得到了投资者的青睐。

其次是区块链行业的矿机和芯片生产商。数字货币矿机的制造主要在于专用芯片。国内的矿机和芯片生产商有深圳烤猫、嘉楠耘智以及比特大陆等。国外的矿机和芯片生产商主要有硅谷比特币创业公司 21 Inc、比特币矿机开发公司 Butterfly Labs、以色列的比特币采矿企业 Spondoolies Tech 等。

以深圳烤猫为例，作为全世界最大的矿团，烤猫曾独占全球比特币挖掘效率近 30%，在许多矿工心里，烤猫就是一个传说。烤猫在 2012 年 7 月年注册成为深证比特泉公司，同年 8 月在全球比特币股票交易所上市，发行 40 万股，其中公众持有 163 962 股，深证比特泉公司持有 236 038 股。不到一年，其公司市值就超过 1.3 亿美元，为公司股东带来大量分红。

最后是研发区块链技术的金融科技类上市公司。在这方面，大家可以关注金融科技类公司在区块链领域的研究开发、参与或设立区块链产业投资基金以及相关并购活动。这方面的公司主要有恒生电子、飞天诚信、广电运通和信雅达等高新技术企业。他们都将会分享区块链技术带来的红利。

11.2.2 巨额资金陆续注入，蓝海变红海

从 2013 年开始，区块链行业已经有比较大的投资进入，比特币也是从这一年开始受到世界各国的关注。随着时间推移，区块链领域的投资也越来越

多。到 2015 年，区块链行业的投资金额达到 4.74 亿美元，比 2014 年增长了 43.5%。截至 2016 年，区块链行业吸引的投资总额已经达到 18 亿美元。

从投资项目上看，资金主要投向了数字货币领域，例如，挖矿、支付、交易平台等。从投资地区分布上看，大多数资金都投在了美国。区块链发展最初的几年里，在中国的投资比较少，但是从 2016 起，中国已经逐渐跟上区块链发展的步伐。大家也能发现，2016 年里，各种区块链峰会、论坛在中国召开，吸引了投资者的眼球。

面对区块链蓝海市场，各方资本纷纷布局。截至 2017 年年初，我国 A 股市场上切入区块链概念的公司已经有 24 家，大部分公司是软件和信息技术提供商。

2016 年以来，以工商银行、平安银行、招商银行、银联等为代表的金融机构都开始布局区块链行业。截至 2016 年年底，平安银行、招商银行、民生银行都已经加入 R3 区块链联盟。除此之外，包括微众银行在内的 20 多家金融机构创建了区块链联盟金联盟，上海华瑞银行也与微众银行合作开发了一套区块链应用系统，用于两家银行微粒贷联合贷款结算与清算。2016 年 9 月底，该系统已经开始试运行。

另外，各大企业也不甘落后。万向集团建立了区块链实验室，华为加入了 Linux 基金会领导的超级账本区块链项目。另外，百度、光大投资管理公司、中金甲子、宜信等机构向一家美国比特币初创公司投资了 6 000 万美元。

从全球范围来看，包括纳斯达克、花旗、Visa 在内的金融行业大咖也向区块链领域大把砸钱，他们联合投资了一家区块链初创公司 Chain，涉及金额高达 3 000 万美元；花旗、摩根大通等金融机构还向一家区块链初创公司 Digital Asset 投资 5 000 万美元。各方都对区块链表示出极大的关注度，区块链技术将从一片巨大的蓝海转变为一片巨大的红海。

区块链红海席卷全球的局势已经基本建立，各种利好即将降临，那些提前进入区块链行业，提供建设区块链经济最原始资本的人，注定会首先品尝到区块链带来的丰厚回报。如果你也准备征战这一红海，那么你需要考虑下面三个问题，内容如图 11-2 所示。

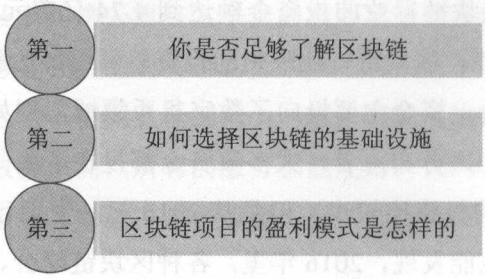


图 11-2　准备进入区块链行业的人需要考虑的三个问题

第一，你是否足够了解区块链。区块链可以用于跟踪任何承载价值的东西，包括金钱、股票、债券以及像房屋和汽车一类的资产。自 2015 年以来，越来越多的区块链项目出现在人们视野中。如果你对区块链在市场和技术方面的表现感到懵懂，说明你对区块链领域还比较陌生，那么你还不能贸然进入区块链领域。

要想分享区块链红海带来的红利，在早期市场中达到投资精、准、快，首先得搞清楚区块链是什么。目前，区块链还没有明确的、公认的定义，但是其显著特性有六个，包括分布式、共同维护、唯一性、可靠、开源、匿名性。

区块链技术应用的研发尚处于早期阶段，而且同时涉及政治、经济、社会、金融、法律、互联网、物联网、人工智能、工业 4.0、大数据、云计算等多个领域，因此深入理解区块链的概念非常重要。

第二，如何选择区块链的基础设施。区块链行业的发展依赖区块链基础设施，否则就会出现根基不稳的问题。作为进入区块链领域的风险投资者，最大的风险和机遇就是对区块链基础设施的选择。互联网的基础设施为个人电脑、智能手机、路由器、服务器、交换机、防火墙等设备，而区块链行业的基础设施主要是实现价值创造、流通和存储等交易行为的区块链应用系统。

截至 2016 年年底，区块链技术已经有 8 年的历史。在这段时间里，很多区块链应用系统还没有来得及问世就直接夭折。统计数据显示，当前公开运行的区块链应有系统将近有 700 个，没有公开的行业专用私链不到 100 个。在这种情况下，投资者可以通过三个指标判断区块链系统的价值高低，内容如图 11-3 所示。

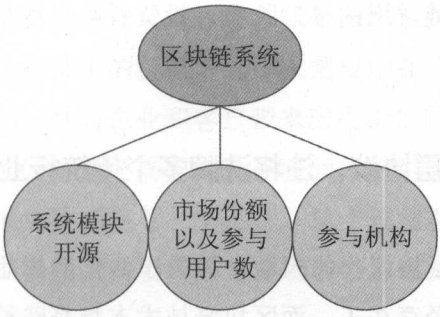


图 11-3　判断区块链系统价值高低的三个指标

1. 系统模块开源

从原则上说，区块链系统的模块都应该开源，就连私链也需要在联盟内部开源。这是实现共识的基本要求，否则就违背了区块链的初衷。

2. 市场份额以及参与用户数

目前，比特币区块链、以太坊区块链以及有待观察的 BTS 都达到了一定的市场份额，有一定数量的参与用户。

3. 参与机构

投资者可以重点关注麻省理工媒体实验室以及 Linux 基金会所推出的“Open Ledger Project”项目，包括 IBM、Cisco、VMware 等设备领域巨头以及众多金融界企业都参与了该项目。

第三，区块链项目的盈利模式是怎样的。投资者看项目最关心的就是盈利模式。对于准备进入区块链行业的投资者来说，可以重点关注一下区块链技术的应用场景和盈利模式。

由于区块链诞生于比特币这种数字货币，所以首先在金融领域中引起了轰动。除此之外，区块链的应用场景还有很多。比如，区块链永久存储信息并通过编程化的代码进行产权确认、计量和交易的优势可以用于产权登记场景。

面对区块链技术，现有的互联网巨头们很难不乱了阵脚。因为区块链的分布式账本特征改变了互联网数据由中心控制者掌控的局面，动摇了互联网公司

的生存基础。在区块链发展的早期阶段，投资者应当尽早布局，尽早进入区块链红海。

11.2.3 作为底层协议，注将洗牌多个传统行业

区块链是一种底层协议，代表着一种去中心化的思想。去中心化的思想在区块链诞生之前就已经存在了。而区块链技术本身是践行去中心化思想的可行技术手段。下面从思想的角度出发，分析区块链技术是如何与传统行业融合，并为企业发展服务的。

传统行业与互联网行业不同，没有太多前沿科技可以吸引大量的风投，也不擅长讲故事。但是，传统行业的发展和转型升级都是他们通过脚踏实地的努力得来的，值得其他行业去学习。

从全局来看，区块链与传统行业的融合有两种方式：一种是传统行业＋区块链；另外一种则是区块链＋传统行业。由于区块链技术本身发展不够成熟，市场上还不存在几个区块链巨头公司，因此采用“区块链＋传统行业”的方式的可能性非常小。

因此，“传统行业主动＋区块链”是更实际的路线。传统行业有自身的诉求，传统企业的客户也有自身的诉求，因此“传统行业＋区块链”不能为了技术而技术。区块链技术是去中心化思想的践行手段，最终应当为传统行业和客户创造新的价值，而创造价值的基础就是解决传统企业的痛点。

第一个需要解决的痛点是传统行业的业务与区块链技术之间缺乏一个桥梁。比如，一家物流公司对区块链技术感兴趣，但是不知道怎么将区块链技术应用在物流行业。

对传统企业的决策者和管理者来说，区块链技术是陌生的，而且技术原理也难以理解。另外，同行业根本没有可以参考的成功应用案例，这是“传统行业＋区块链”需要破解的一大难题。大多数传统企业的决策者可能都是这样想的：我不用区块链技术也能把业务做好，同行也都没有用，那我为什么要用它呢？这种想法是合理的。毕竟企业研发新技术需要投入资金、时间成本以及人力成本，还存在失败风险。

因此，需要一个精通传统企业整体业务，同时也能深刻理解区块链技术的人来做传统行业与区块链技术的桥梁。这个人需要站在一定的业务高度和技术高度上，这样才能找到一种为企业和客户带来应用价值的区块链方案。

这个人尚未出现，或者说还需要很长的时间才能出现，这是必然的。任何新生事物从诞生到发展成熟都需要一个过程，这个过程是技术本身的自我蜕变过程。在这个过程中，新技术需要完成与市场的结合以及市场认知教育，随着商业生态系统一同进化。

在未来，传统行业会以哪种方式＋区块链呢？从区块链技术应用方式的角度来说，“传统行业＋区块链”的方式有两种：一是以破坏性创新的方式构建新的基于区块链技术的商业模式；二是以微创新的方式在企业内部可控的范围内去应用区块链。

无论是哪一种方式，最终的结果都应当是为企业客户创造价值。如果是传统行业的成熟企业，最好的选择是以微创新的方式去应用区块链；如果是传统行业的区块链创业公司，最好的选择是创新商业模式，切入具体细分领域里。因为传统行业是一个成熟的市场，存在大量的既得利益者，区块链创业公司切入这个市场的难度和代价是非常大的，因此选择第二种方式更好一些。

技术的演进是一个长期过程，在这个过程中，传统行业里的企业应当抓住颠覆性技术为企业和客户创造新价值的机遇。在“传统行业＋区块链”的过程中，企业的决策者和管理者应当挖掘区块链的应用场景，与核心员工一起学习和研究区块链技术，掌握区块链的思想。

区块链技术还在持续进化。在这个多变的环境下，你的竞争对手往往不是来自同行业，而是全方位学习新技术，试图通过降维竞争打击你的人。

11.2.4　待开发应用领域多元化，互联网金融领域大有可为

区块链结构主要分为通用协议层、数据层、网络层以及应用层四个层次，每一个层次都蕴含着丰富的投资机遇和创业机会。

通用协议层主要包括隐私保护协议、职能合约协议等。由于开发通用协议需要有极其深厚的技术功底，所以国内还没有人在相关方面创业。随着我国互

联网技术人员的水平不断提升，将会有人成为第一个“吃螃蟹”的人。

区块链结构的数据层主要包括非对称加密技术、分布式数据库等内容。截至2016年7月，国内有超过100家企业从事基于区块链技术的数据登记、储存、公正、安全、识别、认证等业务。

网络层应用的开发主要是做好相关的底层技术，为使用不同区块链技术的人提供一个操作平台。比如，以太坊平台将不同的区块链技术、不同的公司账户聚集到同一个平台上，让他们在以太坊平台上更好地进行操作。

由于开发技术问题，网络层应用的创业是相当困难的，但是回报非常高。一旦创业成功，开发者就可以在上面做各种各样的开发应用，并吸引大量的企业进行注资。对于行业来说，这也是非常大的机遇。目前，只有以太坊是一个成功案例，未来将会有更多企业获得成功。

应用层指的是以分布式网络和分布式账户为基础的各种具体应用。所有需要进行数据记录的行业都可以使用区块链技术来提升工作效率，降低成本，还将会创造一种新的商业模式。应用层的投资是典型的商业化投资，商业利益非常清晰。

从应用层来说，区块链可以用于避免对单一中心的依赖，防止中心的道德腐败；为金融机构提供跨境支付和外汇的解决方案，使结算效率低至3～6秒，比如Ripple；降低银行的交易成本，据风险投资者Anthemis报告，如果采用区块链技术，到2022年以前银行每年可以节省150亿～220亿美元。

区块链技术已在多个领域成立了研发项目，并展现出了大好前景。其中，区块链技术在互联网金融领域的表现备受期待。2016年1月17日，“2015—2016年度微金融50人论坛年会”在北京圆满落幕。多位与会专家表示，区块链技术将在互联网金融领域大有可为，并且成本低于传统模式。

在谈区块链对互联网金融的洗礼之前，我们先看看互联网金融的产品形态。当前互联网金融的产品形态多种多样，下面从四个角度进行分类。

一是互联网金融基础性服务配套设施。互联网金融发展的基础性服务配套设施主要包括以大数据为核心的营销、征信、风控系统、以阿里云为代表的云服务和云计算系统以及以网络支付为代表的三方支付系统。

二是互联网化的传统工具应用服务。互联网化的传统工具应用服务主要包

括供应链金融系统、网络借贷系统、小贷系统、众筹系统、三方支付系统、理财超市系统、大宗商品交易系统、股指期货系统、贵金属实盘系统、财经数据系统、在线博彩系统等。

三是“互联网 + 金融”的具体业态。“互联网 + 金融”的具体业态包括互联网 + 银行、互联网 + 基金、互联网 + 券商、互联网 + 基金、互联网 + 保险等借助互联网开展的新形态。

四是附属服务。互联网金融附属服务包括应用安全检测方面、金融信息安全方面、门户咨询、不良资产处置、咨询服务、法律、资产评估、会计事务所、审计、信用评级、公证与工商金融资质代办服务等。

然而，这些都是现在的金融形态，当区块链技术应用于互联网金融，互联网金融将构建一个“无须第三方中介信任的理想国”。

关于区块链在互联网金融领域的应用，中国人民大学法学院副院长、众筹金融研究院院长杨东认为，比起传统模式，区块链技术在股权交易领域的应用将会有更多优势。

第一，数字股权凭证是一种创新的信任方式。股权转让将会因为独特标识符和数字股权凭证的使用变得更加便捷，有利于增强股权的流动性。另外，数字股权凭证便于监管，也易于扩展支持股权交易的合规性。

第二，区块链记账方式使得股权交易透明，利于公司和持股人追踪信息。基于区块链技术进行的股权交易将会产生新型的数据管理和共享。公司和持股人可以通过数字身份凭证在权限管理体系中读取特定信息。

第三，清算和结算行为更高效。利用区块链技术进行股权交易具有多方协作的优势，这种优势使清算和结算行为更高效。

第四，安全性好、成本低。传统股权交易系统安全性不好，为了保障交易安全，需要从数据库、容灾、防火墙、运维等方面投入大量资金。而利用区块链进行股权交易则可以保证安全，降低交易成本。

区块链在互联网金融领域的应用正在进入新的阶段，各种区块链应用将会越来越深入，互联网金融领域发生的改变也会越来越受人瞩目，然后形成一股极大的新潮流。最终，由互联网金融领域形成的区块链潮流将会影响其他各个领域，直至重新定义这个世界。

Block chain practice

参考文献

[1] 蒋润祥，魏长江．区块链的应用进展与价值探讨 [J]. 甘肃金融，2016（2）:19-21.

[2] 中国人民银行宜宾市中心支行课题组，黎明，梁尤伟．数字货币发展应用及货币体系变革探讨——基于区块链技术 [J]. 西南金融，2016（5）:69-72.

[3] 林晓轩．区块链技术在金融业的应用 [J]. 中国金融，2016（8）:17-18.

[4] 凯文·比勒，丹尼尔·基雅雷拉，赫尔穆特·海德格尔，马修·拉美勒，阿卡什·拉尔，杰瑞德·慕恩，董艳，董丹．区块链技术在资本市场的应用 [J]. 金融市场研究，2016（2）:110-120.

[5] 胡乃静，周欢，董如振．区块链技术颠覆金融未来及在上海金融中心的发展建议 [J]. 上海金融学院学报，2016（3）:31-41.

[6] 袁勇，王飞跃．区块链技术发展现状与展望 [J]. 自动化学报，2016（4）:481-494.

[7] 程华，杨云志．区块链发展趋势与商业银行应对策略研究 [J]. 金融监管研究，2016（6）:73-91.

[8] 益言．区块链的发展现状、银行面临的挑战及对策分析 [J]. 金融会计，2016（4）:46-50.

[9] 张波．国外区块链技术的运用情况及相关启示 [J]. 金融科技时代，2016（5）:35-38.

[10] 张苑．区块链技术对我国金融业发展的影响研究 [J]. 国际金融，2016（5）:41-45.

本书读者对象

- 各领域企业领导、高管
- 金融科技企业工作人员
- 数字货币相关公司工作人员
- 区块链研究以及开发者
- 对区块链以及数字货币感兴趣的其他人群

本书特色

内容全面，结构清晰

本书内容包括区块链的起源、发展、应用以及趋势预测，并重点讲述了区块链在金融领域、物联网领域、大数据领域、医疗领域、教育领域以及公证领域的应用。全书架构清晰，有助于读者形成框架形式的认知。

案例丰富，实战性强

本书加入很多真实且具有代表性的案例，使内容更加生动有趣。而且案例的加入使理论知识不再枯燥无味，读者更容易接受其中的观点。另外，本书理论与实战相结合，非常适合没有接触过区块链的读者阅读，帮助他们快速入门，深入理解区块链的价值。

语言通俗，更接地气

新概念、新技术类的图书总是被作者包装得高大上，看起来非常有范儿，但实质上却提高了读者的理解门槛。而本书倾向于采用通俗易懂的语言为读者解读深奥的理论，让读者轻松理解与区块链相关的理论、应用等知识。

分类建议：经济/前沿趋势
ISBN 978-7-302-47589-7
9 787302 475897 >
定价：49.00元